CENTRAL BANK OF THE UAE

Retail Payment Systems Regulation

CONTENTS

Circular No. : 10/2020

Date : 10/01/2021

To : All System Operators and Settlement Institutions of licensed and/or designated Retail Payment Systems

Subject: Retail Payment Systems

Introduction

The Central Bank is responsible for licensing, designating and overseeing systemically important Retail Payment Systems (RPS) pursuant to the Central Bank Law. The Central Bank Law stipulates criteria and relevant factors based on which the Central Bank will determine whether or not a licensed RPS should be designated and subject to the ongoing oversight of the Central Bank. The policy objective is to ensure that operations of designated RPS are safe, sound, efficient and in compliance with relevant international standards (e.g. the PFMI), and also, would contribute to the financial and payment system stability of the State.

The Central Bank Law expressly sets out the powers of the Central Bank in relation to the licensing, designation and oversight of Financial Infrastructure Systems that are systemically important such as the RPS.

Objective and scope of application:

The objective of this Regulation is to ensure safety and efficiency of Financial Infrastructure Systems and promote efficient and smooth operations thereof.

The Regulation sets out the licensing, designation and oversight framework that the Central Bank intends to follow with respect to the licensing and designation of RPS, and the ongoing oversight of such systems. This Regulation also outlines the major obligations and ongoing requirements of a designated RPS, the powers of the Central Bank in respect thereof, the licensing, designation and ongoing oversight of an RPS.

The scope of this Regulation will cover the systematically important RPS which meet one of the following conditions: (a) the concerned system is operated in the State; or (b) the concerned system has the capacity to provide transfer, clearing or settlement of payment obligations relating to retail activities denominated in the Currency, any currency or any Regulated Medium of Exchange.

This Regulation explains the relevant policies and procedures adopted by the Central Bank with respect to the licensing and designation of RPS. It sets out:

(a) the types of RPS which are likely to be covered by the Regulation; (b) the Central Bank's intended interpretation of the key criteria for designating an RPS; (c) the licensing and designation process; (d) the ongoing requirements of the designated RPS; and

(e) the appeal mechanism in respect of the licensing, designation, suspension and revocation of licensing and/or designation.

The provisions of this Regulation shall not apply to Financial Free Zones and to RPS operating therein unless when expressly provided hereunder.

Article (1): Definitions

1. Central Bank: means the Central Bank of the United Arab Emirates.

2. Central Bank Law: means Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities and its amendments from time to time.

3. Clearing: means the process of transmitting, reconciling and, in some cases, confirming transactions prior to settlement, potentially including the Netting of transactions and the establishment of final positions for settlement.

4. Clearing and Settlement System: means a system established for (a) the clearing or settlement of payment obligations; or (b) the clearing or settlement of obligations for the transfer of book-entry securities, or the transfer of such securities.

5. Currency: means the State's official national currency notes and coins, which its unit is referred as the "Dirham".

6. Default Arrangements: in respect of a Financial Infrastructure System, means the arrangements in place within the system for limiting systemic and other types of risk in the event of a Participant Person appearing to be, or likely to become, unable to meet his obligations in respect of a Transfer Order; and would include any arrangements that have been enforced by the System Operator or Settlement Institution for the following: (1) the Netting of obligations owed to or by a Participant Person; (2) the closing out of open financial position of a Participant Person ; or (3) the realization of collateral securities to secure payment of obligations owed by the Participant Person.

7. Designated System: means any Financial Infrastructure System designated by the Central Bank as systemically important, in accordance with the provisions of the Central Bank Law and the Regulation.

8. Financial Free Zones (FFZ): means free zones subject to the provisions of Federal Law No 8 of 2004, regarding Financial Free Zones, and amending laws.

9. Financial Infrastructure System: means either (1) a Clearing and Settlement System or (2) a Retail Payment System, established, operated, licensed, or overseen by any of the Regulatory Authorities in the State.

10. Grievances & Appeals Committee: means the Committee referred to in Article (136) of the Central Bank Law.

11. License: means a License issued by the Central Bank to an SO and/or SI to operate an RPS in the State. The License shall be valid for a period of five years, unless it is suspended or revoked by the Central Bank.

12. Licensee: means an SO and/or SI that holds a valid License to operate an RPS from the Central Bank.

13. Money's Worth: value added onto an SVF by the customer; value received on the customer's SVF account; and value redeemed by the customer including not only "money" in the primary sense but also other forms of monetary consideration or assets such as values, reward points, Crypto-Assets, or Virtual Assets. For example, a value top-up of an SVF account may take the form of values, reward points, Crypto- Assets, or Virtual Assets earned by the SVF customer from making purchases of goods and services. Similarly, value received on the account of the SVF customer may take the form of an on-line transfer of value, reward points, Crypto-Assets, or Virtual Assets between fellow SVF customers.

14. Netting: in respect of a Clearing and Settlement System, means the conversion of the various obligations owed to or by a Participant Person towards all the other Participant Persons in the system, into one net obligation owed to or by the Participant Person.

15. Operating Rules: means rules set up by the System Operator to cover the operation of a Financial Infrastructure System, including but not limited to, Participant Person account opening and maintenance, contractual relationships with and among Participant Persons, Default Arrangements, payment and settlement processing, Netting and collateral arrangements, authorization and post- transaction processes.

16. Payment System: a Financial Infrastructure System which consists of a set of instruments, procedures, and rules for the transfer of funds between or among Participant Persons.

17. Participant Person: in respect of a Financial Infrastructure System shall mean a Person who is party to or participant of the arrangements for which the system has been established.

18. Person: means a natural or juridical person, as the case may be.

19. Principles of Financial Market Infrastructures (PFMI): means the international standards for financial market infrastructures (i.e. Payment Systems, central securities depositories, securities settlement systems, central counterparties and trade repositories) issued by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities

Commissions (IOSCO). The PFMI are part of a set of 12 key standards that international community considers essential to strengthening and preserving financial stability.

20. Regulated Medium of Exchange: means an instrument or a token that is widely used and accepted in the State as a means of payment for goods and services and regulated by the Central Bank to be a medium of exchange.

21. Regulation: means the Retail Payment Systems Regulation.

22. Regulatory Authorities: means the Central Bank and the Securities & Commodities Authority.

23. Relevant Undertaking: In relation to an SVF, Relevant Undertaking means an undertaking by the Licensee that, upon the use of SVF by the customer as a means for payment for goods and services (which may be or include money or Money's Worth) or payment to another person, and whether or not some other action is also required, the Licensee, or a third party that the SVF issuer has procured to do so, will, in accordance with the Operating Rules: (a) supply the goods or services; (b) make payment for the goods or services; or (c) make payment to the other person, or as the case requires.

24. Retail Payment System (RPS): means any fund transfer system and related instruments, mechanism, and arrangements that typically handles a large volume of relatively low-value payments in such forms as cheques, credit transfers, direct debit, card payment transactions or a Regulated Medium of Exchange.

25. Settlement Institution (SI): means an institution that provides settlement services to a Financial Infrastructure System, settlement accounts in one currency or multi-currency in the Financial Infrastructure System and in certain cases grants access to intraday liquidity to Participant Persons.

26. State: means the United Arab Emirates.

27. Stored Value Facilities (SVF): A facility (other than cash) for or in relation to which a customer, or another person on the customer's behalf, pays a sum of money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets) to the issuer, whether directly or indirectly, in exchange for: (a) the storage of the value of that money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets), whether in whole or in part, on the facility; and (b) the "Relevant Undertaking". SVF includes device-based Stored Value Facility and non-device based Stored Value Facility.

28. System Operator (SO): means a Person responsible for the operation of a Financial Infrastructure System, including the comprehensive management of all risks in the Financial Infrastructure System and ensuring that the operation of the system is in accordance with this Regulation and other relevant regulations issued by the Central Bank.

29. Systemically Important Payment System: means a Financial Infrastructure System which has the potential to trigger or transmit systemic disruptions to the State's monetary and financial stability; this includes, among other things, systems that are the sole Financial Infrastructure System in a jurisdiction or the principal system in terms of the aggregate value of payments, and systems that mainly handle time-critical, high- value payments or settle payments used to effect settlement in other Financial Infrastructure Systems.

30. Transfer: means operationally, the sending (or movement) of funds or securities or of a right relating to funds and securities from one party to another party by (i) conveyance of physical instruments/money; (ii) accounting entries on the books of a financial intermediary; or (iii) accounting entries processed through a funds and/or securities transfer system.

31. Transfer Order: in respect of a Financial Infrastructure System shall mean any of the following instructions: (1) instructions by a Participant Person to make funds available to another Participant Person to be transferred, on a book-entry basis, in the accounts of the Settlement institution for a Clearing and Settlement System; or (2) instructions for discharge from obligation to pay, for the purposes of the Operating Rules of a Clearing and Settlement Systems; or (3) instructions by a Participant Person to either settle an obligation by transferring a book-entry security, or transferring those securities; or (4) instructions by a Participant Person that result in liability or discharge of retail operations payment obligation.

Article (2): Licensing requirements

1. As stipulated in Article (129) (1) (a) of the Central Bank Law, operating an RPS in the State requires a prior License from the Central Bank.

2. The SO and/or SI of the RPS must apply and submit the required information and documents set out in Annex A to the Central Bank for a License if the RPS is in operation in the State.

Article (3): Eligibility and criteria for designation as Systemically Important Financial Infrastructure System

1. As stipulated in Article (126) (2) of the Central Bank Law, if a licensed RPS falls within the eligibility for designation as set out in the aforementioned Article, the Central Bank may designate such RPS as systemically important.

2. Financial Infrastructure Systems which may be covered by the definition of RPS include, but are not limited to, the following systems:

2.1. Electronic funds transfer system: a system that handles transfer of funds which is initiated through a computer system, for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a customer's account. The Central

Bank will not license or designate RPS owned and/or operated by licensed banks (e.g. Internet or mobile banking systems, electronic fund transfer systems, etc.) for serving their own customers

because such RPS are already subject to the Central Bank's prudential supervision of the licensed bank as a whole. However, if a licensed bank provides RPS services to other payment service providers or financial institutions, such RPS may be subject to designation if the RPS falls within the designation criteria.

2.2. Payment card system: a set of functions, procedures, arrangements, rules, and most importantly, a Clearing and Settlement System and network infrastructure that enable a holder of a payment card to effect a payment and/or cash withdrawal transaction with a third party other than the card issuer.

2.3. Clearing and Settlement System for SVF1: a Payment System used to support the SVF business and scheme. An SVF scheme normally requires a Payment System to support their operation. Such a system normally falls within the RPS definition. To avoid regulatory overlap and inducing excess regulatory burden on SVF Licensees, the Central Bank does not intend to designate a Payment System run by a SVF Licensee to support its own SVF business and scheme. It is because the entire SVF business scheme and the related Payment System are already subject to the SVF Regulation, which ensures the safety and soundness of the Payment System.

Detailed regulatory requirements of SVF are set out in the SVF Regulation

including the transfer, clearing and settlement of payment obligations. Nonetheless, if the RPS operated by the SVF Licensee also supports SVF schemes run by other issuers or if a third party operates a Payment System to support other SVF schemes operating in the State, the Central Bank may designate such RPS if it meets the designation criteria.

2.4. Payment gateway: a system that processes, accepts or declines payment transactions on behalf of the merchant secure network connections.

3. In forming an opinion as to whether an RPS satisfies the designation criteria, the Central Bank may consider one or more of the following factors in order to determine whether or not the RPS is a Systemically Important Payment System: -

3.1. The estimated aggregate value of Transfer Orders transferred, cleared or settled through the RPS in a normal business day. The foregoing refers to the total value of individual instructions cleared or settled in the RPS. For established RPS during the transitional period, the estimated value can be worked out with reference to historical data and business plan.

3.2. The estimated average value of Transfer Orders transferred, cleared or settled through the RPS in a normal business day. The foregoing refers to the aggregate value of instructions transferred, cleared or settled through the RPS in a normal business day, divided by the number of

instructions processed.

3.3. The estimated number of Transfer Orders transferred, cleared or settled through the RPS in a normal business day.

3.4. Whether those transactions or the equivalent payment services could be immediately and effectively handled by another Payment System in the State.

3.5. Whether any cross-border activities are involved, including the number of involved countries and the total volume of processed Transfer Orders.

3.6. The estimated number of Participant Persons of the RPS.

3.7. Whether such RPS is linked to any Designated Systems or any Payment System that is licensed or regulated by other Regulatory Authorities in the State.

4. In general, the higher the estimated aggregate value or number of Transfer Orders, the more likely an RPS is material to the financial system of the State and of significant public interest. The number of linkages of an RPS to another Designated System is an important factor that the Central Bank will consider when making a designation decision given the contagion risk to the financial system such linkage could bring.

5. Apart from the above factors, the Central Bank will also consider other factors, for example, in the case of a card payment system, among others, the number of cards issued, the number of card acceptance points. The Central Bank will take a holistic approach in considering these factors, as they complement each other in providing different criteria for assessing the significance of an RPS.

6. The above-mentioned factors are intended to identify an RPS whose proper functioning is material to the monetary or financial stability of the State, or that should be designated, having regard to matters of significant public interest or public order. During the designation process, should the need arise, the Central Bank will discuss with the SO and/or SI of the relevant RPS so as to understand the design and features of the system and assess whether it fulfills the criteria of a Systemically Important Financial Infrastructure System.

Article (4): Designation process

1. The Central Bank will initiate the designation process under the designation framework as stipulated in Article (126) (3) of the Central Bank Law if it considers an RPS is meeting, or is likely to meet the criteria for designation. It is important to note that designation of an RPS does not in any way represent or imply that the Central Bank endorses such system. Designation of an RPS is to provide for such system to be subject to oversight by the Central Bank, with a view to maintaining and promoting the general safety and efficiency of such system.

2. For the Central Bank to determine whether an RPS is eligible to be designated and whether it satisfies the designation criteria for the purposes of this Regulation, the Central Bank will request information or documents regarding the RPS from any Person who is holding, or whom the Central

Bank reasonably believes holds such information or documents or is a SO and/or SI of the RPS or a Participant Person in the RPS. This power to request information or documents applies to RPS, individuals or corporations established, located or incorporated in the State and/or outside the State. The Central Bank will coordinate with any competent Regulatory Authority in the State or other competent authorities in other jurisdictions for the purpose of requesting and securing such information and documents.

3. Generally speaking, the Central Bank will seek to request information or documents as set out in the Annexes of this Regulation and may, where necessary, seek additional information as is required in order to assist the Central Bank in making such determination. The types of information or documents that the Central Bank will require might vary from RPS to RPS.

4. During the designation process, the Central Bank may discuss with the SO and/or SI of such system where necessary to understand the features and the design of the system and determine the RPS's eligibility for designation.

5. The time for the designation process may vary depending on the particular situation of each case, including the nature and complexity of the prospective designated RPS, the completeness of information and documents submitted to the Central Bank.

6. The SO and/or SI of the designated RPS may submit a grievance against the designation decision by applying to the Grievances & Appeal Committee. Details on the appeal mechanism as set out in Article (11) of this Regulation.

7. If the Central Bank intends to designate any of the RPS licensed by a competent Regulatory Authority in the State or competent regulatory authorities in other jurisdictions as systemically important RPS, the Central Bank shall implement the process provided for under Article (126) (6) of the Central Bank Law.

RPS deemed to have been licensed and designated

8. As stipulated in Article (126) (5) of the Central Bank Law, the RPS established, developed, and/or operated by the Central Bank are deemed to have been licensed and designated.

9. The RPSs that are deemed to have been designated are required to observe all the obligations and requirements imposed on designated RPSs under this Regulation in the same manner as other designated RPSs.

Article (5): Cooperation with relevant regulatory authorities

1. As part of the designation process for RPS established and/or licensed by another Regulatory Authority in the State or by relevant regulatory authorities in other jurisdictions, the Central Bank

may agree with the relevant regulatory authority which parts of this Regulation, where relevant, may not apply to concerned designated RPS to avoid additional regulatory burden on the SO and SI of the RPS.

2. The Central Bank will rely on co-operative oversight with the relevant regulatory authority of a designated RPS operating in the State or in other jurisdictions, in accordance with articles

(28) and (127) (2) of the Central Bank Law and the cooperative framework set out in the PFMI.

Article (6): Revocation of License and designation

Grounds for revocation

1. As stipulated in Article (128) of the Central Bank Law, the Central Bank may revoke the License of an RPS if the RPS is unable to carry out its operations in compliance with the provisions of the Central Bank Law or this Regulations.

2. As stipulated in Article (126) (7) of the Central Bank Law, the Central Bank may revoke the designation of an RPS if the RPS has ceased to be, or is likely to cease being a Systemically Important Financial Infrastructure System or an RPS whose proper functioning is material to the monetary or financial stability of the State.

Revocation process

3. The Central Bank will prepare a review report on whether a licensed and/or designated RPS satisfies the revocation criteria under this Regulation. If the Central Bank intends to revoke the License and/or the designation of a RPS, the Central Bank will notify in writing the SO and/or SI of the RPS or the regulatory authority where the RPS is licensed so that such authority can notify the SO and/or SI of the system of the intention of the Central Bank to revoke the License and/or the designation. The notice needs to state the grounds on which the revocation is to be made and specify in the notice a period of not less than twenty (20) working days from the date of notification, during which the SO and/or SI of the system may be heard, or may make written justifications, as to why the grounds for revocation stated in the notice are not valid

4. If any SO and/or SI of the licensed and/or designated RPS wish to be heard or to make written justifications, it should make such a request to the Central Bank in writing before the revocation takes effect, giving reasons as to why the grounds for revocation specified in the notice have not been established. After reviewing the reasons given by the SO and/or SI, the Central Bank will determine whether the Licensee and/or designation should be revoked. In the course of reviewing the matter, the Central Bank may meet with the SO and/or SI of the License and/or designated RPS should such need arise.

5. If the Central Bank decides to proceed to revoke the License and/or designation of the RPS, the Central Bank will notify the SO and/or SI of the RPS of the Central Bank’s decision in writing.

6. The SO and/or SI may object to the Central Bank's decision to revoke the License and/or the designation of the RPS and provide justifications for such objection by applying to the Grievances & Appeals Committee as provided by the Central Bank Law.

7. The Central Bank, if it considers that any of the RPS licensed by another Regulatory Authority in the State or the relevant regulatory authorities in other jurisdictions is no longer meeting the designation criteria, may request the concerned regulatory authority, via an official notice, to revoke the License and/or designation of the RPS.

8. In all cases, the revocation of the License and/or designation of the RPS shall not affect any transaction cleared and settled in the concerned RPS prior to the effective date of revocation.

Article (7): Settlement finality

1. In accordance with Article (131) of the Central Bank Law settlement finality is "the discharge of an obligation by a transfer of funds that has become irrevocable and unconditional". Specifically, "settlement finality" refers to the abrogation of all rights otherwise existing at law that would allow the reversal of a Transfer Order effected through, or proceeding within, an RPS.

2. Article (131) (1) of the Central Bank Law grants finality to all transactions conducted through a Financial Infrastructure System, therefore rendering the same final, irrevocable and irreversible, in any of the cases provided for thereunder. Besides finality in respect of Transfer Orders, the Central Bank Law also provides legal certainty on the Netting arrangements in a designated RPS.

3. If Netting has been effected in an RPS that meets any of the designation conditions refers to in Article (126) (2) of the Central Bank Law, the SO and/or SI needs to take into consideration the Netting of obligations of insolvent or bankrupt parties in Article (133) of the Central Bank Law.

4. In addition, the preservation of rights in underlying transactions and obligation of Participant Person to notify of insolvency are set out in Article (134) and Article (135) of the Central Bank Law respectively.

Article (8): Ongoing requirements of designated Retail Payment Systems

Principal Requirements

1. The SO and/or SI of a designated RPS, are required to ensure compliance with the following:

1.1. RPS must comply with any instructions issued by the Central Bank and any relevant international standards (e.g. PFMI), and ensure proper and continued functioning of the designated RPS; and

1.2. RPS must provide the information required by the Central Bank or where SO and/or SI consider it appropriate for achievement of the Central Bank objectives.

2. The Central Bank may exempt the SO and/or SI or a Participant Person of a designated RPS in a general or specific manner, from the provisions of this Regulation.

3. The Central Bank may appoint experts and advisors specialized in Financial Infrastructure Systems to assist the Central Bank in performing its duties and functions in accordance with this Regulation.

Detailed requirements

Principal requirements

4. Upon designation, a designated RPS is required to comply with the ongoing requirements imposed under this Regulation and the relevant provisions of PFMI (see Article (9) for detail). Failure to comply with any of those requirements would expose the concerned party to possible sanctions provided for under the Central Bank Law. The principal requirements include: -

4.1. Submission of particulars – the Central Bank requires any SO and/or SI of a newly designated RPS to inform the Central Bank in writing of the designation particulars within fourteen (14) working days after the notification of designation, including the name, place of business, postal address and electronic mail address, as well as the aspects of the management or operations of the system. For any SO and/or SI which is a corporation, the names and personal particulars of the directors, chief executive (if any) and shareholders of the corporation are similarly required to be submitted to the Central Bank. Details of any subsequent change in any of those particulars are to be notified to the Central Bank in writing within fourteen (14) days of the change taking effect.

4.2. Compliance with safety and efficiency requirements - the general requirements include safe and efficient operation of the RPS, the establishment of appropriate Operating Rules, the existence of adequate compliance arrangements, and the availability of appropriate financial resources.

4.3. Submission of information or documents - the Central Bank may request information or documents relating to a designated RPS from the SO and/or SI of, or the Participant Person in, the RPS when performing the oversight functions under this Regulation. The SO and/or SI of, or the Participant Person in the designated RPS to whom a request is made is required to submit the information or documents within the period specified in the request.

4.4. The Central Bank may, at any time, with a short prior notice to the SO and/SI concerned, examine any books, accounts or transactions of the SO and/or SI of a designated RPS when performing the oversight functions.

4.5. The Central Bank may require the SO and/or SI of, or the Participant Person in, a designated RPS to submit to the Central Bank a report prepared by one or more auditors on matters that the Central Bank requires for discharging or exercising its duties and powers under this Regulation.

4.6. The Central Bank may direct the SO and/or SI of a designated RPS to take any action necessary to bring the RPS into compliance with any of the requirements under this Regulation. Such a direction will specify the Central Bank's concerns and the action(s) to be taken, include a statement of the respect in which the Central Bank considers the designated RPS not be in compliance with a requirement under this Regulation and specify the period within which the direction is to be complied with.

4.7. The Central Bank may, by notice in writing, direct the SO and/or SI of a designated RPS to take any action the Central Bank considers necessary to bring the RPS into compliance with any of the requirements under this Regulation.

Obligation of SO and SI to notify the Central Bank of certain events

5. The SO and/or SI of a designated RPS must notify the Central Bank of the occurrence of any of the following events as soon as practicable after that occurrence:

5.1. An event or irregularity that impedes or prevents access to, or impairs the usual operations of, the designated RPS or its settlement operations.

5.2. Any material function of the SO and/or SI that is outsourced.

5.3. Any civil or criminal proceeding instituted against the SO and/or SI, whether in the State or elsewhere.

5.4. The SO and/or SI being unable to meet any of the financial, statutory, contractual or other obligations of the SO and/or SI.

5.5. Any disciplinary action taken against the SO and/or SI by any regulatory authority, whether in the State or elsewhere.

5.6. Any change of the chief executive officer or senior management of the SO and/or SI.

Governance arrangements

6. The SO and/or SI of the designated RPS must have clearly defined and documented organizational arrangements, such as ownership and management structure. Each should operate with appropriate segregation of duties and internal control arrangements so as to reduce the risk of mismanagement and fraud.

7. The SO and/or SI of the designated RPS must have effective measures and controls to ensure compliance with this Regulation. Appropriate processes must be in place to ensure that rules and procedures as well as the contractual relationships with its Participant Persons are valid and enforceable. These include clear rules and procedures to govern transfer, clearing and settlement for both domestic and cross-border transactions (if applicable).

Compliance

8. The SO and/or SI of the designated RPS are required to perform a periodic self-assessment or independent assessment of its compliance with this Regulation and the relevant principles of the PFMI set out in Article (9) of this Regulation. Such assessment must be done at least every 24 months. Its internal auditors, internal compliance officer or appointed independent assessor should perform such assessment as part of their on-going duties and provide the Central Bank with a copy of their compliance report. Assessment reports submitted to the Central Bank by the SO and/or SI of the designated RPS are confidential and shall not be disclosed to any third party unless the approval of the Central Bank is obtained.

Financial requirement

9. The financial condition of the SO and/or SI of the designated RPS must be sound and viable, and subject to ongoing review and monitoring by the senior management of the SO and/or SI.

Participation criteria

10. The SO and/or SI of the designated RPS must have an established process for considering applications to become its Participant Person. The SO and/or SI of the designated RPS must have procedures in place to allow prospective Participant Persons to access or obtain the information necessary to determine whether to apply to become a Participant Person.

11. The general eligibility and participation criteria should be disclosed to genuine applicants upon request.

Transparency, interoperability and competition

12. The SO and/or SI of the designated RPS shall not establish or impose any operational policies, procedures and arrangements that will prevent operational transparency or interoperability among Payment Systems, and competition among market players. The SO and/or SI of the designated RPS must observe and comply with all relevant laws, codes of practice and guidelines applicable to their payment activities and services in the State.

13. If the Central Bank considers the interoperability between the RPS and other Payment System(s) would be in the interest of the public or the Participant Persons of systems involved, it may direct the SO and/or SI of the RPS involved to enter into arrangements to enable the interoperability among the systems involved or to adopt any common standards.

14. The relevant fees and charges must be documented and communicated clearly to the Participant Persons.

15. The SO and/or SI of the designated RPS must inform affected Participant Persons of changes to its operational procedures and arrangements that materially affect such parties' financial risk, operational risk, data security risk and legal risk in the State.

Rules and procedures

16. The SO and/or SI of the designated RPS must have proper Operating Rules to enable its Participant Persons to obtain sufficient information regarding their respective rights and obligations associated with their participation in the RPS. Such rights and obligations must be clearly defined and disclosed to the Participant Persons.

17. Operating Rules of the RPS must be complete, up-to-date and readily available to all Participant Persons. Participant Persons must also be duly informed of any relevant changes in the Operating Rules.

18. The SI must establish rules and procedures to enable final settlement to take place no later than the end of the intended settlement date. The related rules and procedures must also ensure certainty in terms of circumstances under which Transfer Orders effected through the RPS are to be regarded as settled for the purposes of the RPS.

19. The liabilities of Participant Persons for any loss arising from unauthorized use of the RPS and the arrangements to handle any disputes over Participant Persons' liability with respect to unauthorized transactions must be clearly set out in the rules and procedures.

Operational efficiency

20. The SO and/or SI of the designated RPS should provide convenient and efficient payment services to its Participant Persons, and ensure that the RPS can process transactions at a speed which is efficient and complies with the RPS' committed service level.

Operational reliability and business continuity

21. The SO and/or SI of the designated RPS must have sound and prudent management, administrative, accounting and control procedures managing the financial and non- financial risks to which it reasonably considers it may be exposed.

22. The SO and/or SI of the designated RPS must conduct risk analysis on new payment activity or service. In addition, where it reasonably believes that there has been a change of relevant circumstances, the SO and/or SI of the designated RPS should perform a review on the risk profile of existing activities and services to assess risks relating to security and business continuity.

23. The SO and/or SI of the designated RPS must seek to ensure that it has an adequate number of properly trained and competent personnel to operate its system at a level it considers appropriate in all situations that it considers are reasonably foreseeable.

24. The SO and/or SI of the designated RPS should provide its Participant Persons with information it reasonably considers relevant to fraud awareness in the context of the operation of its payment activities and services. The SO and/or SI of the designated RPS should provide

Participant Persons with education it reasonably considers relevant to fraud awareness and the proper use or processing of the RPS to reduce the risk of fraud so that the Participant Persons can educate and promote the awareness of their customers accordingly.

25. The SO and/or SI of the designated RPS must have comprehensive, rigorous and well-documented operational and technical procedures to address reasonable operational reliability, the integrity of its network and the timeliness of transactions in the face of malfunctions, system interruption and transmission failures or delays. The SO and/or SI of the designated RPS must also have in place a reasonable, effective, well-documented and regularly-tested business contingency plan addressing system functionality in the event of unforeseen interruption.

26. The SO and/or SI of the designated RPS must have a thorough due diligence and management oversight process for managing its outsourcing relationships, if any, that it considers may impact the operation of its payment activities and services. The liabilities and responsibilities between the SO and/or SI of the designated RPS and its outsourcing service providers must be clearly defined.

27. The SO and/or SI of the designated RPS must design its technical system for payment activities and services with sufficient capacity to enable its ongoing operations, which should be monitored periodically and upgraded on a periodic basis.

28. The SO and/or SI of the designated RPS must have sufficient clearing and settlement arrangements to enable efficient, reliable and secure operation of the RPS.

29. The SO and/or SI of the designated RPS must review periodically its security objectives, policies and operational services.

30. The SO and/or SI of the designated RPS must develop well-defined procedures to respond to

payment activity or service security-related incidents. The procedures should encompass a consistent and systematic approach in handling an incident.

31. As a follow-up to each security-related incident materially affecting the Participant Persons, the SO and/or SI of the designated RPS should initiate a confidential post-incident assessment of the situation by the parties it considers appropriate having regard to the nature and the root cause of the incident, weaknesses leading to the incident and other potentially vulnerabilities underlying the incident.

Safety

32. The SO and/or SI of the designated RPS must adopt appropriate and commercially reasonable technical security measures and procedural safeguards to protect the security of its system. The SO and/or SI of the designated RPS should also consider adopting international technical security standards where appropriate.

33. The required measures must include the building and maintenance of a secure network, including conditions to install and maintain firewalls to protect data, and a change of vendor-supplied default system passwords and other security passwords.

34. The implemented measures must protect data through the entire life cycle of a transaction, particularly on control measures to access data, procedures for storing Participant Persons' transaction data, and disposal of Participant Persons' transaction information after use.

35. The designated RPS must use and regularly update anti-virus software to maintain secure systems and applications, and take proper measures to manage cyber security risk effectively, including the capability to keep pace with the trends of cyber-attacks.

36. In addition, the SO and/or SI of the designated RPS must have mechanisms which enable them to monitor on an ongoing basis attempted security breaches that may compromise its systems and data. There should be measures to control access and to regularly monitor and test the operation networks. There must be a policy that addresses information security for all related parties, such as employees and contractors.

37. The SO and/or SI of the designated RPS must conduct periodic security reviews of its system. Such reviews could be performed either by the SO and/or SI of the designated RPS or, at its (or the Central Bank's) discretion, by an independent party appointed by it.

Data Security and Integrity

38. The SO and/or SI of the designated RPS are responsible for the security and integrity of all payment data and records maintained or controlled by it. The SO and/or SI of the designated RPS should ensure that the Participant Persons have, rules and procedures to safeguard the necessary confidentiality of all data and records in its control, including customer and transaction information. The SO and/or SI of the designated RPS should adopt generally accepted industry and international data security standards that it considers to be applicable to its operations.

39. The SO and/or SI of the designated RPS must establish and maintain policies and procedures for the recovery of transaction data that is necessary for its daily operation in the event of system failure.

Incident Reporting

40. The SO and/or SI of the designated RPS must report to the Central Bank of any incident (such as data security breaches) that may have a material and adverse impact on its operation or other Systematically Important Payment Systems in the State.

41. Where action has been taken under Default Arrangements of a designated RPS by the SO and/or SI in respect of a Participant Person in the RPS, the Central Bank may direct the SO and/or SI of a designated RPS to give information relating to the default to any official nominated by the Central Bank. The nominated official is responsible for assessing and examining any matter arising

out of or connected with the default of the Participant Person in that RPS. The liabilities of Participant Persons for any loss arising from the default of the Participant Person and the arrangements to handle any disputes over Participant Persons' liability with respect to default transactions should be clearly set out in the rules and procedures.

Article (9): Compliance with Principles of Financial Market Infrastructures Requirements

1. The Committee on Payment and Market Infrastructures (CPMI) and the Technical Committee of the International Organization of Securities Commissions (IOSCO) have set forth a set of PFMI. PFMI aims to assist central banks, market regulators, and other relevant authorities in enhancing safety and efficiency in payment, clearing, settlement, and recording arrangements, and more broadly, limiting systemic risk and fostering transparency and financial stability. (details of PFMI are available in the two websites: www.bis.org and www.iosco.org).

2. Another objective of PFMI is to harmonize and, where appropriate, strengthen the existing international standards and risk management practice for Financial Infrastructure Systems such as RPS that are systemically important.

3. A poorly designed and operated systemically important RPS can contribute to and exacerbate systemic crises if the risks of the RPS are not adequately managed. The financial shocks, as a result, could be passed from one Participant Person to another Participant Person as well as a separate Systematically Important Payment System. The effects of such a disruption could extend well beyond the RPS and their Participant Persons, threatening the stability of domestic financial markets and the broader economy.

4. Against this backdrop, the SI and/or SO should robustly manage the risks of their systematically important RPS to ensure its safety and promote financial stability. In addition, a systemically important RPS should not only be safe, but also efficient. Efficiency refers generally to the use of resources by SO and/or SI and their Participant Persons in performing their functions. Safe and efficient systemically important RPS contributes to well-functioning financial markets and economy.

5. The Central Bank requires any designated RPS to observe and comply with the relevant principles in the PFMI, in addition to the compliance with the ongoing requirements set out in Article (8) of this Regulation. Moreover, the Central Bank may consider imposing higher requirements than PFMI for the designated RPS either on the basis of specific risks posed by the RPS or as a general policy.

6. The SO and/or SI must apply the relevant principles on an ongoing basis in the operation of their RPS and business, including when reviewing their own performance, assessing or proposing new services, or proposing changes to risk controls.

7. In aligning this regulation with leading international practice, RPS must comply with the relevant principles set out in the following paragraphs.

8. Principle 1: Legal basis – a systemically important RPS must have a well-founded, clear, transparent, with a high degree of legal certainty, and an enforceable legal framework for each material aspect of its activities.

9. Principle 2: Governance – a systemically important RPS must have governance arrangements that are clear and transparent, promote the safety and efficiency of the RPS, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.

10. Principle 3: Framework for the comprehensive management of risks – a systemically important RPS must have a sound risk management framework for comprehensively managing legal, credit, liquidity, operational, and other risks.

11. Principle 4: Credit risk – a systemically important RPS must effectively measure, monitor, and manage its credit exposures to Participant Persons and those arising from its payment, clearing and settlement processes. The systematically important RPS must maintain sufficient financial resources to cover its credit exposures to each Participant Person fully with a high degree of confidence.

12. Principle 5: Collateral – a systemically important RPS that requires collateral to manage its or its Participant Persons' credit exposure should accept collateral with low credit, liquidity, and market risks. A systematically important RPS should also set and enforce appropriately conservative haircuts and concentration limits.

13. Principle 6: Liquidity risk – a systemically important RPS must effectively measure, monitor, and manage its liquidity risk. A systemically important RPS should maintain sufficient liquid resources in all relevant currencies to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the Participant Person and its affiliates that would generate the largest aggregate liquidity obligation for the systemically important RPS in extreme but plausible market conditions.

14. Principle 7: Money settlement – a systemically important RPS should conduct its money settlements in central bank money where practical and available. If central bank money is not used, a systemically important RPS should minimize and strictly control the credit and liquidity risk arising from the use of commercial bank money.

15. Principle 8: Participant-default rules and procedures – a systemically important RPS must have effective and clearly defined rules and procedures to manage a Participant Person default. These rules and procedures should be designed to ensure that the systemically important RPS can take timely action to contain losses and liquidity pressures and continue to meet its obligations.

16. Principle 9: General business risk – a systemically important RPS must identify, monitor, and manage its general business risk and hold sufficient liquid net assets funded by equity to cover potential general business losses so that it can continue operations and services as a going concern if those losses materialize. Further, liquid net assets should at all times be sufficient to ensure a recovery or orderly wind- down of critical operations and services.

17. Principle 10: Operational risk – a systemically important RPS must identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systemically important RPS should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the systemically important RPS's obligations, including in the event of a wide-scale or major disruption.

18. Principle 11: Access and participation requirements – a systemically important RPS should have objective, risk-based, and publicly disclosed criteria for participation, which permit fair and open access.

19. Principle 12: Tiered participation arrangements – a systemically important RPS should identify, monitor, and manage the material risks to the systemically important RPS arising from tiered participation arrangements.

20. Principle 13: Financial market infrastructure links – a systemically important RPS that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks.

21. Principle 14: Efficiency and effectiveness – a systemically important RPS should be efficient and effective in meeting the requirements of its Participant Persons and the markets it serves.

22. Principle 15: Communication procedures and standards – a systemically important RPS should use, or at a minimum accommodate, relevantinternationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement, and recording.

23. Principle 16: Disclosure of rules, key procedures, and market data – a systemically important RPS must have clear and comprehensive rules and procedures and must provide sufficient information to enable Participant Persons to have an accurate understanding of the risks, fees, and other material costs they incur by participating in the systemically important RPS. All relevant rules and key procedures should be adequately disclosed.

Article (10): Enforcement and sanctions

1. Violation of any provision of this Regulation or committing any of the violations provided for under the Central Bank Law may subject SI and/or SO to administrative and financial sanctions and penalties as deemed appropriate by the Central Bank.

Article (11): Appeal mechanism

1. For the purposes of this Regulation, the relevant Central Bank's decisions that may be subject to appeal before the Grievances & Appeals Committee include: -

1.1. licensing and designation of RPS;

1.2. revocation of License and designation of RPS; and

1.3. any Central Bank's actions undertaken against a violating Person.

2. Under the Regulation, any Person aggrieved by any of the decisions set out in paragraph 1 of this Article may refer the decision to the Grievances & Appeals Committee in writing for review.

3. Any person who intends to refer any of the relevant decisions of the Central Bank to the Grievances & Appeals Committee is required to do so in writing to the Central Bank stating the grounds on which the review is sought.

Article (12): Transition period

1. A one-year transitional period will commence on the date the Regulation comes into force. System Operators and Settlement Institutions of existing RPS operating in the State may continue operating throughout the transitional period without being regarded as contravening this Regulation. Nevertheless, they are required to obtain a license from the Central Bank to operate their RPS before the expiration of the transition period.

2. If the Central Bank considers that a Financial Infrastructure System fulfills the criteria for designation as provided for under the Central Bank Law, the Central Bank shall have the power to require any such system to obtain a license within a reasonable period to be determined by the Central

Bank prior to the expiration of the transition period.

Article (13): Interpretation of Regulation

1. The Regulatory Development Division of the Central Bank shall be the reference for interpretation of the provisions of this Regulation.

Article (14): Publication & application

1. This Regulation shall be published in the Official Gazette in both Arabic and English and shall come into effect one month from the date of publication. In case of any discrepancy between the Arabic and the English, the Arabic version will prevail.

Abdulhamid M. Saeed Alahmadi Governor of the Central Bank of the UAE

ANNEX A

Information or documents that may be requested for licensing of RPS operating in the State under this Regulation

1. Name of clearing and settlement system to which the designated RPS relates.

2. Name of SO / SI.

3. Legal form (body corporate, partnership, etc.).

4. Country of incorporation or formation.

5. Date of incorporation or formation.

6. Registered office.

7. Principal place of business.

8. Contact details (names, physical and email addresses).

9. Aspects of the management or operations of the system for which the entity is responsible.

10. Organization chart of your company.

11. A copy of the Operating Rules of the Payment System.

12. Details of the type of activities and/or services offered by the RPS.

13. Details of the constitution, structure, nature of business, ownership and management of the RPS, the SO and the SI.

14. Details of the design and function and external system interfaces of the RPS, including details specifying the point at which a Transfer Order takes effect as having

been entered into the RPS and of the point after which a Transfer Order may not be

revoked by a Participant Person or any other party.

15. A copy of the last three annual reports, if any, and the financial statements (with any auditor's reports) for the current financial year of the RPS, the SO and/or the SI.

16. The basis for membership of or participation in the RPS System (i.e. admission criteria) and a list of the current members of or Participant Persons in the RPS.

17. Tariff information and schedule.

18. Names of the SO and/or SI, if any, of the RPS and whether the SO and/or SI are also Participant Persons in the RPS under the Operating Rules of the System. Legal contracts or documents between the SO and/or the SI in relation to the RPS (for instance, documents which show the co-operation between the SO and/or SI, such as MoUs between them on data security, and the functional specifications of the linkages between the computer systems and networks between them that makes the system works.).

19. Name and contact details of the Person to whom questions relating to the designation of the RPS should be directed.

ANNEX B

Information or documents that may be requested under this Regulation

1. A copy of the Operating Rules of the Payment System.

2. Details of the type of activities and/or services offered by the RPS.

3. Details of the constitution, structure, nature of business, ownership and management of the RPS, the SO and the SI.

4. Details of the design and function and external system interfaces of the RPS, including details specifying the point at which a Transfer Order takes effect as having been entered into the RPS and of the point after which a Transfer Order may not be revoked by a Participant Person or any other party.

5. A copy of the last three annual reports, if any, and the financial statements (with any auditor's reports) for the current financial year of the RPS, the SO and/or the SI.

6. The basis for membership of or participation in the RPS System (i.e. admission criteria) and a list of the current members of or Participant Persons in the RPS.

7. Tariff information and schedule.

8. Names of the SO and/or SI, if any, of the RPS and whether the SO and/or SI are also Participant Persons in the RPS under the Operating Rules of the System. Legal contracts or documents between the SO and/or the SI in relation to the RPS (for instance, documents which show the co-operation between the SO and/or SI, such as MoUs between them on data security, and the functional specifications of the linkages between the computer systems and networks between them that makes the system works.).

9. Details of the types, volume and values of Transfer Orders processed by the RPS.

10. Detailed business contingency plan.

11. Name and contact details of the Person to whom questions relating to the designation of the RPS should be directed.

For overseas systems, the following additional information may be required: -

1. Name of each of the relevant regulators where the RPS is regulated by one or more regulatory authorities not within the State jurisdiction.

2. An outline of any laws and other regulatory requirements relating to the operations of the RPS, if regulated by a regulatory authority not within the State jurisdiction.

3. Evidence of the RPS' compliance with any applicable laws and regulatory requirements of a jurisdiction outside State, which may include comments from home supervisory authority on the RPS's compliance with any applicable laws and regulatory requirements of a jurisdiction outside State.

CENTRAL BANK OF THE U.A.E

Retail Payment Services and Card Schemes Regulation

CONTENTS		
Subject		**Page**

Circular No. : **15/2021**
Date : **06/06/2021**
To : **Providers of Retail Payment Services and Card Schemes in the United Arab Emirates**

Subject : **Retail Payment Services and Card Schemes Regulation**

Introduction

The Regulation ('RPSCS Regulation') lays down the rules and conditions established by the Central Bank for granting a License for the provision of Retail Payment Services. The Retail Payment Services are digital payment services in the State and comprise nine categories, namely Payment Account Issuance Services, Payment Instrument Issuance Services, Merchant Acquiring Services, Payment Aggregation Services, Domestic and Cross-border Fund Transfer Services, Payment Token Services, Payment Initiation Services and Payment Account Information Services. It also requires Card Schemes to obtain a License from the Central Bank and sets out the conditions for granting such License as well as the ongoing obligations of Card Schemes. The Central Bank has furthermore been given the right to receive information on the fees and charges of Card Schemes, and regulate such fees and charges if the Central Bank considers it appropriate. In addition, proper contractual arrangements are required between Banks or other Payment Service Providers providing Payment Account Issuance Services, on one hand, and Payment Service Providers providing Payment Initiation and Payment Account Information Services, on the other hand. Payment Service Providers wishing to participate in wages distribution and be given access to the Wages Protection System are subject to a set of on-going requirements.

The Central Bank Law requires providing money transfer services, electronic retail payments, and digital money services to be subject to a licensing regime administered by the Central Bank and provides the statutory basis for the powers of the Central Bank in relation to the licensing and ongoing supervision of Payment Service Providers and Card Schemes.

Scope and Objectives

This Regulation sets out the requirements concerning:

- conditions for granting and maintaining a License for the provision of Retail Payment Services;
- rights and obligations of Retail Payment Service Users and Payment Service Providers;
- proper contractual arrangements allowing Payment Service Providers providing Payment Initiation and Payment Account Information Services to access Payment Accounts held with Banks and other Payment Service Providers providing Payment Account Issuance Services;
- conditions for granting a License to Card Schemes;
- conditions for participating and obtaining an access to the Wages Protection System;
- powers of the Central Bank with regard to the supervision of Payment Service Providers and the on-going reporting requirements for Card Schemes.

In exercising its powers and functions under this Regulation, the Central Bank has regard to the following objectives:

- ensuring the safety, soundness and efficiency of Retail Payment Services;

- adoption of effective and risk-based licensing requirements for Payment Service Providers;
- promoting the reliability and efficiency of Card Schemes as well as public confidence in Card-based Payment Transactions;
- promoting innovation and creating a level playing field for market participants; and
- reinforcing the UAE's status as a leading payment hub in the region.

Exclusions

This Regulation shall not apply to the following:

1. Payment Transactions involving Stored Value Facilities;
2. Transactions involving Commodity or Security Tokens;
3. Transactions involving Virtual Asset Tokens;
4. Payment Transactions involving Remittances;
5. Currency exchange operations where the funds are not held on a Payment Account;
6. Any service other than Payment Initiation and Payment Account Information Service, including (but not limited to) any of the following:
    6.1. services, provided by any technical service provider that supports the provision of any payment service, but does not at any time enter into possession of any money under that payment service;
    6.2. the service of processing or storing data;
    6.3. any information technology security, trust or privacy protection service;
    6.4. any data or entity authentication service;
    6.5. any information technology service;
    6.6. the service of providing a communication network; and
    6.7. the service of providing and maintaining any terminal or device used for any payment service.
7. Payment Transactions carried out within a payment system or securities settlement system between Payment Service Providers and settlement agents, central counterparties, clearing houses, central banks or other participants in such system including central securities depositories;
8. Payment Transactions and related services between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a Payment Service Provider other than an undertaking belonging to the same group; and
9. Any other relevant activity that may be designated by the Central Bank.

Article (1): Definitions

1. **Agent:** means a juridical Person providing Retail Payment Services on behalf of a Payment Service Provider.
2. **AML/CFT:** means Anti-Money Laundering and Combating the Financing of Terrorism.
3. **AML Law:** means Decree Federal Law No.(20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations and Cabinet Decision No.(10) of 2019 Concerning the Implementing Regulation of Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as may be amended from time to time, and any instructions, guidelines and notices issued by the Central Bank relating to their implementation or issued in this regard.
4. **Annex I:** means the list of Retail Payment Services that a Payment Service Provider may provide subject to the requirements of this Regulation.
5. **Annex II:** means the Guidance on the best practices for technology risk and information security.

6. **Annex III:** means the minimum level of information to be reported by Card Schemes to the Central Bank.

7. **Applicant:** means a juridical Person duly incorporated in the State in accordance with Federal Law No. 2 of 2015 on Commercial Companies and as provided for under Article (74) of the Central Bank Law, which files an Application with the Central Bank for the granting of a License for the provision of one or more Retail Payment Services, operation of a Card Scheme or the modification of the scope of a granted License.

8. **Application:** means a written request for obtaining a License for the provision of one or more Retail Payment Services submitted by an Applicant which contains the information and documents specified in this Regulation or by the Central Bank, and is in the form specified by the Central Bank's Licensing Division, including a written request for obtaining a modification to the scope of a granted License.

9. **Auditor:** means an independent juridical Person that has been appointed to audit the accounts and financial statements of a Payment Service Provider in accordance with Article (10) (7).

10. **Bank:** any juridical person licensed in accordance with the provisions of the Central Bank Law, to primarily carry on the activity of taking deposits, and any other Licensed Financial Activities.

11. **Beneficial Owner:** means the natural person who owns or exercises effective ultimate control, directly or indirectly, over a Retail Payment Service User (client) or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or legal arrangement.

12. **Branded:** means having any digital name, term, sign, logo, symbol or combination thereof that is capable of differentiating the Card Scheme under which Payment Transactions are executed.

13. **Board:** means the board of directors of an Applicant, Payment Service Provider or a Card Scheme in accordance with applicable corporate law.

14. **Business Day:** means a day other than Friday, Saturday, public holiday or other non-working holiday or day in the State.

15. **Card-based Payment Transactions:** means a service based on a Card Scheme's infrastructure and business rules to make Payment Transactions by means of any card, telecommunication, digital or IT device or software if this results in a debit or a credit card transaction.

16. **Card Issuer:** means a category of Payment Service Provider providing a Payer with a Payment Instrument to initiate and process the Payer's Card-based Payment Transactions.

17. **Cardholder:** means a Person who holds a Payment Instrument, physical or otherwise, issued by a Card Issuer based on a contract for the provision of an electronic payment instrument.

18. **Card Scheme:** means a single set of rules, practices and standards that enable a holder of a Payment Instrument to effect the execution of Card-based Payment Transactions within the State which is separated from any infrastructure of payment system that supports its operation, and includes the Card Scheme Governing Body. For the avoidance of doubt, a Card Scheme may be operated by a private or Public Sector Entity.

19. **Card Scheme License:** means a License for operating as a Card Scheme, as referred to in Article (18).

20. **Card Scheme Governing Body:** means the juridical Person responsible and/or accountable for the functioning and operation of a Card Scheme.

21. **Category I License:** means a License for the provision of the Retail Payment Services referred to in Article (3) (2).

22. **Category II License** means a License for the provision of the Retail Payment Services referred to in Article (3) (3).

23. **Category III License** means a License for the provision of the Retail Payment Services referred to in Article (3) (4).

24. **Category IV License** means a License for the provision of the Retail Payment Services referred to in Article (3)

(5).

25. **Central Bank:** means the Central Bank of the United Arab Emirates.

26. **entral Bank Law:** means the Decretal Federal Law No. (14) of 2018 Regarding the Central Bank and Organization of Financial Institutions and Services, as may be amended or substituted from time to time.

27. **Co-Branded:** means having the inclusion of at least one payment brand and one non-payment brand on the same Payment Instrument.

28. **Controller:** means a natural or juridical Person that alone or together with the Person's associates has an interest in at least 20% of the shares in a Payment Service Providers or is in a position to control at least 20% of the votes in a Payment Service Provider.

29. **Commodity Token**: means a type of Crypto- Asset that grants its holder an access to a current or prospective product or service, and is only accepted by the issuer of that token. Commodity token can also be referred to as utility token

30. **Complaint:** Means an expression of dissatisfaction by a consumer with a product, service, policy, procedure or actions by the licensed financial institution that is presented to an Employee of the licensed financial institution in writing or verbally.

31. **Cross-Border Fund Transfer Service:** means a Retail Payment Service for the transfer of funds in which the Payment Service Providers of the Payer and the Payee are located in different jurisdictions/countries.

32. **Crypto-Assets:** means cryptographically secured digital representations of value or contractual rights that use a form of Distributed Ledger Technology and can be transferred, stored or traded electronically.

33. **Customer Due Diligence or CDD:** means the process of identifying or verifying the information of a Retail Payment Service User or Beneficial Owner, whether a natural or legal person or a legal arrangement, and the nature of its activity and the purpose of the business relationship and the ownership structure and control over it.

34. **Custodian Services**: means the safekeeping or controlling, on behalf of third parties, of Payment Tokens, the means of access to such tokens, where applicable in the form of private cryptographic keys.

35. **Data Breach:** means an intrusion into an IT system where unauthorized disclosure or theft, modification or destruction of Cardholder or Retail Payment Service User data is suspected and such is likely to result in a loss for the Cardholder or Retail Payment Service User.

36. **Data Subject:** means an identified or identifiable natural Person who is the subject of Personal Data.

37. **Digital Money Services:** means, for the purposes of this Regulation, the business activity related to the provision of Payment Token Services.

38. **Distributed Ledger Technology:** means a class of technologies that supports the distributed recording of encrypted data across a network and which is a type of decentralized database of which there are multiple identical copies distributed among multiple participants and accessible across different sites and locations, and which are updated in a synchronized manner by consensus of the participants, eliminating the need for a central authority or intermediary to process, validate or authenticate transactions or other types of data exchanges.

39. **Domestic Fund Transfer Service:** means the Retail Payment Service of accepting money for the purpose of executing, or arranging for the execution of Payment Transactions between a Payer in the State and a Payee in the State.

40. **Electronic Payment Service:** means any and each of the Retail Payment Services listed in points (1) to (4) and (8) to (9) of Annex I.

41. **Employer:** means a Person using the Wages Protection System for the payment of wages.

42. **Exchange House:** means an exchange business that has been licensed under the Regulations re Licensing and

Monitoring of Exchange Business.

43. **Exempted Person:** means any Person who is exempted from the requirement to hold a License as per Article (2) of this Regulation.

44. **Facilitating the Exchange of Payment Tokens:** means a Retail Payment Service related to establishing or operating a Payment Token exchange, in a case where the person that establishes or operates that exchange, for the purposes of an offer or invitation made or to be made on that Payment Token exchange, to buy or sell any Payment Token in exchange for Fiat Currency or Payment Token, whether of the same or a different type, comes into possession of any Fiat Currency or Payment Token, whether at the time that offer or invitation is made or otherwise.

45. **FATF:** an inter-government body which sets international standards that aim to prevent global money laundering and terrorist financing activities.

46. **Fiat Currency:** means a currency that is controlled by the respective central bank, has the status of legal tender and is required to be accepted within a given jurisdiction.

47. **Financial Free Zones:** means free zones subject to the provisions of Federal Law No (8) of 2004, regarding Financial Free Zones, as may be amended or supplemented from time to time.

48. **Four Party Card Scheme**: means a Card Scheme in which Card-based Payment Transactions are made from the payment account of a Payer to the payment account of a payee through the intermediation of the scheme, an issuer (on the payer's side) and an acquirer (on the Payee's side).

49. **Framework Agreement:** means a payment service agreement for the provision of Retail Payment Services which governs the future execution of individual and successive Payment Transactions and which may contain the terms and conditions for opening a Payment Account**.**

50. **Group:** means a corporate group which consists of a parent entity and its subsidiaries, and the entities in which the parent entity or its subsidiaries hold, directly or indirectly, 5% or more of the shares, or are otherwise linked by a joint venture relationship.

51. **Legal Form:** means the legal form of Applicants established in accordance with Article (74) of the Central Bank Law.

52. **Level 2 Acts:** means any written act that may be adopted or issued by the Central Bank complementing the implementation of this Regulation, such as, without being limited to, rules, directives, decisions, instructions, notices, circulars, standards, and rulebooks.

53. **License:** means a License issued by the Central Bank to an Applicant to provide Retail Payment Services or operate a Card Scheme in the State. The License is valid unless it is withdrawn, suspended or revoked by the Central Bank.

54. **Licensed Financial Activities:** means the financial activities subject to Central Bank licensing and supervision, which are specified in Article (65) of the Central Bank Law.

55. **Major Regulatory Requirement:** means any requirement of this Regulation or Level 2 Acts the violation of which is capable of compromising and/or negatively affecting the attainment of the Central Bank's objectives pursued under this Regulation, as determined at the discretion of the Central Bank.

56. **Management:** means the Applicant, Payment Service Provider, Agent and Card Scheme's senior officers that are involved in the daily management, supervision and control of the business services of the entity, typically including the chief executive officer, his or her alternate(s) and each person directly reporting to that officer. The chief executive officer and his or her alternate(s) shall be a natural person who are ordinarily residing in the State whereas the remaining members of Management shall be based in the State unless the Central Bank allows otherwise.

57. **Means of Distance Communication:** means a method which may be used for the conclusion of a payment services

agreement without the simultaneous physical presence of the Payment Service Provider and the Retail Payment Service User.

58. **Merchant:** means a Person who accepts Payment Instruments as a mode of payment for the purchase and sale of goods and services.

59. **Merchant Acquirer:** means a category of Payment Service Provider providing Merchant Acquiring Services.

60. **Merchant Acquiring Service:** means a Retail Payment Service provided by a Payment Service Provider contracting with a Payee to accept and process Payment Transactions, which results in a transfer of funds to the Payee.

61. **Money Transfer Services:** means the Domestic and Cross-border Fund Transfers Services, excluding Remittances.

62. **Money's Worth:** means value added onto an SVF by the customer; value received on the customer's SVF account; and value redeemed by the customer including not only "money" in the primary sense but also other forms of monetary consideration or assets such as values, reward points, Crypto-Assets, or Virtual Assets. For example, a value top-up of an SVF account may take the form of values, reward points, Crypto- Assets, or Virtual Assets earned by the SVF customer from making purchases of goods and services. Similarly, value received on the account of the SVF customer may take the form of an on-line transfer of value, reward points, Crypto-Assets, or Virtual Assets between fellow SVF customers.

63. **Payment Account:** means an account with a Payment Service Provider held in the name of at least one Retail Payment Service User which is used for the execution of Payment Transactions.

64. **Payment Account Information Service:** means a Retail Payment Service to provide consolidated information on one or more Payment Accounts held by a Retail Payment Service User with either another Payment Service Provider or with more than one Payment Service Providers. For the avoidance of doubt, the Payment Account Information Service does not involve the holding of Retail Payment Service User's funds at any time.

65. **Payment Account Issuance Service:** means a Retail Payment Service, other than Domestic and Cross-border Fund Transfer Services, enabling (i) the opening of a Payment Account; (ii) cash to be placed on a Payment Account; (iii) cash to be withdrawn from a Payment Account; and (iv) all necessary operations for operating a Payment Account. The Payment Account is only used for holding fund/cash in transit and not allowed to store and maintain fund/cash.

66. **Payment Aggregation Service:** means a Retail Payment Service facilitating e-commerce websites and Merchants to accept various Payment Instruments from the Retail Payment Service Users for completion of their payment obligations without the need for Merchants to create a separate payment integration system of their own. Payment aggregation facilitates Merchants to connect with Merchant acquirers; in the process, they receive payments from Retail Payment Service Users, pool and transfer them on to the Merchants after a time period.

67. **Payment Data:** means any information related to a Retail Payment Service User, including financial data and excluding Personal Data.

68. **Payment Initiation Service:** means a Retail Payment Service to initiate a Payment Order at the request of the Retail Payment Service User with respect to a Payment Account held at another Payment Service Provider. For the avoidance of doubt, the Payment Initiation Service does not involve the holding and maintenance of Payer's funds at any time.

69. **Payment Instrument:** means a personalized device(s), a payment card and/or set of procedures agreed between the Retail Payment Service User and the Payment Service Provider, and used in order to initiate a Payment Order.

70. **Payment Instrument Issuance Service:** means a Retail Payment Service related to the provision of a Payment Instrument to a Retail Payment Service User which enables it to initiate Payment Orders as well as the Processing of the Retail Payment Service User's Payment Transactions.

71. **Payment Service Provider:** means a legal Person that has been licensed in accordance with this Regulation to

provide one or more Retail Payment Services and has been included in the Register as per Article (73) of the Central Bank Law.

72. **Payment Token Issuing**: means a Retail Payment Service related to the issuing of Payment Tokens by a Payment Service Provider. For the avoidance of doubt, Payment Tokens may not be offered to the public or segments thereof unless the Payment Service Provider issuing the Payment Tokens has obtained a Category I License, drafted a White Paper in respect of those Payment Tokens and received an approval by the Central Bank prior to offering such tokens to the public.

73. **Payment Token:** means a type of Crypto-Asset that is backed by one or more Fiat Currencies, can be digitally traded and functions as (i) a medium of exchange; and/or (ii) a unit of account; and/or (iii) a store of value, but does not have legal tender status in any jurisdiction. A Payment Token is neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Payment Token. For the avoidance of doubt, a Payment Token does not represent any equity or debt claim.

74. **Payment Token Buying**: means the buying of Payment Tokens in exchange for any Fiat Currency or Payment Token.

75. **Payment Token Selling:** means the selling of Payment Tokens in exchange for any Fiat Currency or Payment Token.

76. **Payment Token Services:** means the Retail Payment Services consisting of any of the following activities related to Payment Tokens: (i) Payment Token Issuing; (ii) Payment Token Buying; (iii) Payment Token Selling; (iv) Facilitating the Exchange of Payment Tokens; (v) enabling payments to Merchants and/or enabling peer-to-peer payments; and (vi) Custodian Services. For the avoidance of doubt, a Payment Service Provider may provide only one of the Retail Payment Services referred to in points (v) and (vi); if it wishes to provide both and allows Retail Payment Service Users to redeem the Payment Tokens with any Fiat Currency under a contractual arrangement, it must comply with the respective SVF requirements.

77. **Payment Transaction:** means an act initiated by the Payer or on his behalf or by the Payee of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the Payer and the Payee.

78. **Payee:** means a Person who is the intended recipient of funds which have been the subject of a Payment Transaction.

79. **Payer:** means a Person who holds a Payment Account and allows a Payment Order from that Payment Account, or, where there is no Payment Account, a Person who gives a Payment Order.

80. **Person** means any natural or legal Person.

81. **Personal Data:** means any information which are related to an identified or identifiable natural Person.

82. **Processing:** means Payment Transaction processing necessary for the handling of an instruction, including clearing and settlement, between the Merchant Acquirer and the Card Issuer.

83. **Promotion:** means any form of communication, by any means, aimed at inviting or offering to enter into an agreement related to any Retail Payment Service. For the avoidance of doubt, any Person that has been mandated to provide or engage in Promotion activities by a Person providing Retail Payment Services without holding a License shall not be held liable under this Regulation.

84. **Public Sector Entity:** means the Federal Government, Governments of the Union's member Emirates, public institutions and organizations.

85. **Register:** means the Register referred to in Article (73) of the Central Bank Law.

86. **Regulation:** means the Retail Payment Services and Card Schemes Regulation.

87. **Remittance:** means the receipt of funds from a Payer without any Payment Accounts being created in the name of

the Payer or the Payee.

88. **Reserve of Assets**: means the pool of Fiat Currencies that are legal tender backing the value of a Payment Token.

89. **Retail Payment Service:** means any business activity set out in Annex I.

90. **Retail Payment Service User:** means a Person who intends to make use of or makes use of a Retail Payment Service in the capacity of a Payer, Payee or both.

91. **Sensitive Payment Data:** means data, including personalized security credentials which can be used to carry out unauthorized activities. For the purposes of Payment Initiation and Payment Account Information Services, the name of the Payment Account owner and Payment Account number shall not constitute Sensitive Payment Data.

92. **Single Retail Payment Agreement:** means an agreement which governs the execution of an individual Payment Transaction.

93. **State:** means the United Arab Emirates.

94. **Security Token:** means a type of Crypto-Asset that provides its holder with rights and obligations that represent a debt or equity claim against the issuer of that token.

95. **Stored Value Facility or SVF**: means a facility (other than cash) for or in relation to which a Customer, or another person on the Customer's behalf, pays a sum of money (including Money's Worth such as values, reward points, Crypto- Assets or Virtual Assets) to the issuer, whether directly or indirectly, in exchange for: (a) the storage of the value of that money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets), whether in whole or in part, on the facility; and (b) the "Relevant Undertaking". SVF includes Device- based Stored Value Facility and Non-device based Stored Value Facility.

96. **Third country:** means a country other than the UAE.

97. **Three Party Card Scheme**: means a Card Scheme in which the scheme itself provides Merchant Acquiring and Payment Instrument Issuing Services and Card-based Payment Transactions are made from the Payment Account of a Payer to the Payment Account of a Payee within the Card Scheme. When a Three Party Card Scheme licenses other Payment Service Providers for the issuance of Card-based Payment Instruments or the Merchant Acquiring of Card-based Payment Transactions, or both, or issues Card-based Payment Instruments with a co-branding partner or through an agent, it is considered to be a Four Party Card Scheme.

98. **UAE:** means the United Arab Emirates.

99. **Unauthorized Payment Transaction:** means a Payment Transaction for the execution of which the Payer has not given consent. Consent to execute a Payment Transaction or a series of Payment Transactions shall be given in the form agreed between the Payer and the Payment Service Provider. Consent to execute a Payment Transaction may also be given via the Payee or the Payment Initiation Service Provider.

100. **Virtual Assets:** A Virtual Asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual Assets do not include digital representations of Fiat Currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

101. **Virtual Assets Service Providers:** Virtual Asset Service Provider means any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between Virtual Assets and Fiat Currencies; (ii) exchange between one or more forms of Virtual Assets; (iii) transfer of Virtual Assets; (iv.) safekeeping and/or administration of Virtual Assets or instruments enabling control over Virtual Assets; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a Virtual Asset.

102. **Virtual Asset Token**: means a type of Crypto- Asset that can be digitally traded and functions as (i) a unit of account; and/or (ii) a store of value. Although some Virtual Asset Tokens may be accepted as a means of payment, they are generally not accepted as a medium of exchange, may not have an issuer and do not have legal tender status

in any jurisdiction. A Virtual Asset Token is neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Virtual Asset Token. For the avoidance of doubt, a Virtual Asset Token does not represent any equity or debt claim, and it is not backed by any Fiat Currency.

103. **Virtual Asset Token Services**: means any of the following services: (i) enabling peer-to-peer Virtual Asset Token transfers, and (ii) custodian services of Virtual Asset Tokens.

104. **Wages Protection System or WPS:** means a reconciliation system implemented at the Central Bank aimed at providing a safe, secure, efficient and robust mechanism for streamlining the timely and efficient payment of wages.

105. **Wire Transfer:** means any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person

106. **WPS Payment Account:** means a WPS account opened in the infrastructure of the Central Bank and held for the purposes of holding and payment of wages.

107. **WPS Payment Account Holder:** means a holder of a Payment Account held with a Payment Service Provider who has been given access to the Wages Protection System for the purpose of executing transfers of wages.

108. **White Paper:** means a detailed description in Arabic and English of: (i) the Payment Service Provider issuing a Payment Token and a presentation of the main participants involved in the project's design and development; (ii) a detailed description of the project and the type of Payment Token that will be offered to the public; (iii) the number of Payment Tokens that will be issued and the issue price; (iv) a detailed description of the rights and obligations attached to the Payment Token and the procedures and conditions for exercising those rights; (v) information on the underlying technology and standards applied by the Payment Service Provider issuing the Payment Token allowing for the holding, storing and transfer of those Payment Tokens; (vi) a detailed description of the risks relating to the Payment Service Provider issuing Payment Tokens, the Payment Tokens, the offer to the public and the implementation of the project, and other disclosures that the Central Bank may specify; (vii) detailed description of the Payment Service Provider's governance arrangements, including a description of the role, responsibilities and accountability of the third-parties responsible for operating, investment and custody of the Reserve of Assets, and, where applicable, the distribution of the Payment Tokens; (viii) a detailed description of the Reserve of Assets; (ix) a detailed description of the custody arrangements for the Reserve Assets, including the segregation of the assets; (x) in case of an investment of the Reserve of Assets, a detailed description of the investment policy; and (xi) information on the nature and enforceability of rights, including any direct redemption right or any claims that holders of Payment Tokens may have on the Reserve of Assets or against the Payment Service Provider issuing the Payment Tokens, including how such rights may be treated in insolvency procedures. For the avoidance of doubt, the White Paper shall be written in a simple, easy to understand and non-misleading language, and shall be dated. The White Paper shall be endorsed by the Payment Service Provider's Management and published on the Payment Service Provider's website after receipt of an approval by the Central Bank.

Article (2): Licensing

1. No Person shall provide or engage in the Promotion within the State of any of the Retail Payment Services set out in Annex I without obtaining a prior License from the Central Bank unless this Person is an exempted Person.

Exempted Persons

2. Banks licensed in accordance with the Central Bank Law shall be deemed licensed to provide Retail Payment Services and shall therefore be exempt from the prohibition laid down in paragraph (1). Nevertheless, Banks shall be required to notify the Central Bank in writing if they intend to provide the Retail Payment Services referred to in points (3) to (4) and (7) to
(9) of Annex I and obtain a No Objection Letter prior to commencing the provision of such services. Banks are exempted from the No Objection Letter requirement and any licensing requirements for providing the Retail

Payment Services referred to in points (1), (2), (5) and (6) of Annex I.

3. For the avoidance of doubt, Banks providing Retail Payment Services other than the Retail Payment Services referred to in points (1), (2), (5) and (6) of Annex I, shall be required to comply only with the requirements set out in Article (11) on Payment Token Services, Article (12) on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, Article (13) on Technology Risk and Information Security, and Article (14) on Obligations Towards Retail Payment Service Users.
4. Finance companies licensed in accordance with the finance companies Regulation shall be exempt from the prohibition laid down in paragraph (1) for the service of issuance of credit cards. For the avoidance of doubt, except issuance of credit cards, finance companies that intend to provide Retail Payment Services shall be required to obtain a prior License from the Central Bank.
5. The Central Bank may request from a Person or Exempted Person the provision of any information or documentation that it considers necessary to determine the eligibility for exemption or continued exemption, respectively.
6. The Central Bank reserves the right to withdraw an exemption granted under this Article 2.

Article (3): License Categories

1. A Person that intends to provide Retail Payment Services shall apply for one of the following categories of License:
    1.1. Category I License;
    1.2. Category II License;
    1.3. Category III License; and
    1.4. Category IV License
2. An Applicant shall apply for a Category I License where it intends to provide one or more of the following Retail Payment Services:
    2.1. Payment Account Issuance Services;
    2.2. Payment Instrument Issuance Services;
    2.3. Merchant Acquiring Services;
    2.4. Payment Aggregation Services;
    2.5. Domestic Fund Transfer Services;
    2.6. Cross-border Fund Transfer Services; and
    2.7. Payment Token Services.
3. An Applicant shall apply for a Category II License where it intends to provide one or more of the following Retail Payment Services:
    3.1. Payment Account Issuance Services;
    3.2. Payment Instrument Issuance Services;
    3.3. Merchant Acquiring Services;
    3.4. Payment Aggregation Services;
    3.5. Domestic Fund Transfer Services; and
    3.6. Cross-border Fund Transfer Services.
4. An Applicant shall apply for a Category III License where it intends to provide one or more of the following Retail Payment Services:
    4.1. Payment Account Issuance Services;

4.2. Payment Instrument Issuance Services;

4.3. Merchant Acquiring Services;

4.4. Payment Aggregation Services; and

4.5. Domestic Fund Transfer Services.

5. An Applicant shall apply for a Category IV License where it intends to provide one or all of the following Retail Payment Services:

5.1. Payment Initiation Services; and

5.2. Payment Account Information Services.

Article (4): License Conditions

1. To be granted a License, an Applicant shall, at the time of submitting an Application:

1.1. fulfil the Legal Form;

1.2. meet the respective initial capital requirements per License Category specified in Article (6); and

1.3. provide the necessary documents and information specified in the Central Bank application form as provided by the Licensing Division.

2. In addition to the requirements set out in paragraph (1) to be granted a Category I License, an Applicant shall, at the time of submitting an Application, provide a list of all Payment Tokens that it intends to issue and obtain a legal opinion on the assessment for all Payment Tokens.

3. In addition to the requirements set out in paragraph (1), to be granted a Category IV License, an Applicant shall, at the time of submitting an Application, hold a professional indemnity insurance as per Article (10) paragraphs (14) to (16).

Article (5): Licensing Procedure

1. The licensing of Applicants shall be subject to the procedure envisaged in the Central Bank's Licensing Guidelines.
2. The Management of an Applicant is encouraged to meet with the Central Bank's Licensing Division before submitting a formal Application.

Article (6): Initial Capital

1. An Applicant shall hold, upon being granted a License by the Central Bank, initial capital as per the below:

1.1. for obtaining a Category I License:

1.1.1. initial capital of at least three (3) million Dirhams where the monthly average value of Payment Transactions amounts to ten
(10) million Dirhams or above; or

1.1.2. initial capital of at least one and a half (1.5) million Dirhams where the monthly average value of Payment Transactions amounts to less than ten (10) million Dirhams.

1.2. for obtaining a Category II License:

1.2.1. initial capital of at least two
(2) million Dirhams where the monthly average value of Payment Transactions amounts to ten
(10) million Dirhams or above; or

1.2.2. initial capital of at least one
(1) million Dirhams where the monthly average value of Payment Transactions amounts to less than ten
(10) million Dirhams.

1.3. for obtaining a Category III License:

1.3.1. initial capital of at least one (1) million Dirhams where the monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above; or

1.3.2. initial capital of at least five hundred thousand (500,000) Dirhams where the monthly average value of Payment Transactions amounts to less than ten (10) million Dirhams.

1.4. for obtaining a Category IV License: initial capital of at least one hundred thousand (100,000) Dirhams regardless of the monthly average value of Payment Transactions.

2. An Applicant shall provide information to the Central Bank on the source(s) of funds that constitute the initial capital as per paragraph (1).

Calculation Method

3. The monthly average value of Payment Transactions referred to in paragraph (1) shall be calculated on the basis of the moving average of the preceding (3) months or, where such data does not exist at the time of being granted a License by the Central Bank, on the basis of the business plan and financial projections provided.

Article (7): Aggregate Capital Funds

1. A Payment Service Provider shall hold and maintain at all times aggregate capital funds that do not fall below the initial capital requirements laid down in Article (6), taking into consideration the applicable License category.

2. The Central Bank may impose aggregate capital funds requirements higher than the ones referred to in paragraph (1) if, taking into consideration the scale and complexity of the Payment Service Provider's business, it considers such higher requirements essential to ensuring that the Payment Service Provider has the ability to fulfil its obligations under this Regulation.

3. Where the monthly average value of Payment Transactions calculated in accordance with Article (6) (3) exceeds the Payment Transaction threshold of ten (10) million Dirhams in (3) consecutive months, Payment Service Providers shall report this fact to the Central Bank and become automatically subject to the higher aggregate capital funds requirements determined by the Central Bank under paragraph (2).

4. The aggregate capital funds referred to in paragraph (1) shall be comprised of one or more of the capital items provided for in paragraphs (5) and (6).

Capital Items

5. A Payment Service Provider's aggregate capital funds shall consist of:

5.1. Paid-up capital;

5.2. Reserves, excluding revaluation reserves; and

5.3. Retained earnings.

6. The following items shall be deducted from the aggregate capital funds:

6.1. Accumulated losses; and

6.2. Goodwill.

Article (8): Control of Controllers

1. A Person shall not become a Controller in a Payment Service Provider without obtaining a prior approval from the Central Bank.

2. The Central Bank shall grant an approval under paragraph (1) if it considers that:

2.1. having regard to the likely influence of the Controller, the Payment Service Provider will remain compliant with the requirements of this Regulation and Level 2 Acts; and

2.2. the Controller meets the fit and proper requirements specified by the Central Bank.

3. The approval under paragraph (2) may be granted subject to any conditions that the Central Bank may impose on the Person, including but not limited to:

3.1. conditions restricting the Person's disposal or further acquisition of shares or voting powers in the Payment Service Provider; and

3.2. conditions restricting the Person's exercise of voting power in the Payment Service Provider.

Article (9): Principal Business

1. The principal business of a Payment Service Provider shall be the provision of the Retail Payment Service(s) for which it has been granted a License.

2. Where a Payment Service Provider intends to provide ancillary service(s) falling outside the scope of its License, it shall obtain the approval of the Central Bank prior to commencing the provision of such service(s).

3. The Central Bank requires prior approval for the provision of any ancillary service(s) by a Payment Service Provider, and may require a Payment Service Provider that intends to provide ancillary service(s), to create a separate entity for the provision of such services, if it believes that the conduct of the ancillary activities may have a negative impact on the Payment Service Provider's ability to comply with the requirements of this Regulation and
Level 2 Acts.

Article (10): On-Going Requirements

Corporate Governance

1. Payment Service Providers must comply with the below requirements on corporate governance.

2. Payment Service Providers must have and maintain effective, robust and well-documented corporate governance arrangements, including a clear organizational structure with well-defined, transparent and consistent lines of responsibility.

3. The corporate governance arrangements referred to in paragraph (2) must be comprehensive and proportionate to the nature, scale and complexity of the Retail Payment Services provided, and shall contain, at a minimum:

3.1. an organization chart showing each division, department or unit, indicating the name of each responsible individual accompanied by a description of the respective function and responsibilities;

3.2. controls on conflicts of interest;

3.3. controls on integrity and transparency of the Payment Service Provider's operations;

3.4. controls to ensure compliance with applicable laws and regulations;

3.5. methods for maintaining confidentiality of information; and

3.6. procedures for regular monitoring and auditing of all corporate governance arrangements.

Risk Management

4. Payment Service Providers must have and maintain robust and comprehensive policies and procedures to identify, manage, monitor and report the risks arising from the provision of Retail Payment Services to which they are or might become exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures.

5. Payment Service Providers' risk management policies and procedures shall be:

5.1. kept up-to-date;

5.2. reviewed annually; and

5.3. proportionate to the nature, scale and complexity of the Retail Payment Services provided.

6. Payment Service Providers must establish a risk management function, an internal audit function and a compliance function.

Accounting and Audit

7. Payment Service Providers must appoint an Auditor to audit on an annual basis:

    7.1. the financial statements or consolidated financial statements of the Payment Service Provider prepared in accordance with the accepted accounting standards and practices; and

    7.2. the systems and controls of the Retail Payment Services provided by the Payment Service Provider, separately from any audit on non-Retail Payment Services.

8. Upon request by the Central Bank, the appointed Auditor shall submit, directly or through the Payment Service Provider, a report of the audit in a form and within a timeframe acceptable to the Central Bank.

9. In addition to the report of audit, the Central Bank may request from the Auditor to:
    9.1. submit any additional information in relation to the audit, if the Central Bank considers it necessary;

    9.2. enlarge or extend the scope of the audit;

    9.3. carry out any other examination.

Record Keeping

10. Payment Service Providers shall keep all necessary records on Personal and Payment Data for a period of (5) years from the date of receipt of such data, unless otherwise required by other applicable laws or the Central Bank.

Notification Requirements

11. Where any material change affects the accuracy and completeness of information provided in an Application, the Applicant or Payment Service Provider, as the case may be, shall immediately notify the Central Bank of such change and provide all necessary information and documents.

12. A Payment Service Provider shall immediately notify the Central Bank of any violation or potential violation of a Major Regulatory Requirement of this Regulation or Level 2 Acts.

13. A Payment Service Provider shall immediately notify the Central Bank if it becomes aware that any of the following events have occurred or are likely to occur:

    13.1. any event that prevents access to or disrupts the operations of the Payment Service Provider;

    13.2. any legal action taken against the Payment Service Provider either in the State or in a Third Country;

    13.3. the commencement of any insolvency, winding up, liquidation or equivalent proceedings, or the appointment of any receiver, administrator or provisional liquidator under the laws of any country;

    13.4. any disciplinary measure or sanction taken against the Payment Service Provider or imposed on it by a regulatory body other than the Central Bank, whether in the State or in a Third Country;

    13.5. any change in regulatory requirements to which it is subject beyond those of the Central Bank, whether in the State or in a Third Country; and

    13.6. any other event specified by the Central Bank.

Professional Indemnity Insurance

14. Payment Service Providers providing Payment Initiation and Payment Account Information Services shall hold a professional indemnity insurance whose amount shall be decided upon by the Central Bank.

15. The professional indemnity insurance of Payment Service Providers providing Payment Initiation Services referred to in paragraph (14) shall cover these Payment Service Providers' liabilities for Unauthorized Payment Transactions and non-execution, defective or late execution of Payment Transactions.

16. The professional indemnity insurance of Payment Service Providers providing Payment Account Information Services referred to in paragraph (14) shall cover these Payment Service Providers' liability vis-à-vis the Payment Service Provider providing Account Issuance Services or the Retail Payment Service User resulting from non-authorized or fraudulent access to or non-authorized or fraudulent use of

Payment Account information.

Article (11) Payment Token Services

1. This Article (11) is without prejudice to other provisions of this Regulation that are relevant to Payment Service Providers providing Payment Token Services.

2. For the avoidance of doubt, Payment Token Services do not include Security Token, Commodity Token and Virtual Asset Token and the provision of services associated with the same.

3. Security Token and Commodity Token fall within the jurisdiction of the Securities and Commodities Authority and as such are regulated by the Securities and Commodities Authority.

4. Virtual Asset Tokens, although may be accepted as a means of payment, are not generally accepted as a medium of exchange due to the lack of stability and high volatility in their market value. As a result, any services associated with Virtual Asset Tokens, including Virtual Asset Token Services, fall outside the scope of this Regulation.

Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations

5. Payment Token Services shall be considered to carry high money laundering and terrorist financing risk due to their speed, anonymity and cross-border nature. In line with the FATF standards, Payment Services Providers providing Payment Token Services shall undertake risk assessment and take appropriate measures to manage and mitigate the identified risks in accordance with applicable legal and regulatory requirements. Payment Service Providers providing Payment Token Services shall comply with the FATF Guidance for a Risk-based Approach to Virtual Assets and Virtual Assets Service Providers, as may be supplemented from time to time, or any related standards or guidance in assessing and managing risks in Payment Token Services.

Technology Risk and Information Security

Security Requirements

6. A Payment Service Provider providing Payment Token Services shall have a good understanding of the security risks and vulnerabilities of each Payment Token provided. It shall carry out a security risk assessment for each Payment Token.

Cyber Security Risk

7. Payment Service Providers providing Payment Token Services whose monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above shall regularly assess the necessity to perform penetration and cyber- attack simulation testing. Coverage and scope of testing shall be based on the cyber security risk profile, cyber intelligence information available, covering not only networks (both external and internal) and application systems but also social engineering and emerging cyber threats. A Payment Service Provider shall also take appropriate actions to mitigate the issues, threats and vulnerabilities identified in penetration and cyber-attack simulation testing in a timely manner, based on the impact and risk exposure analysis.

Specific Obligations for Providing Retail Payment Service on Payment Tokens

Reserve of Assets

8. Payment Service Providers issuing Payment Tokens shall keep and maintain at all times a Reserve of Assets per category of Payment Token issued.

9. Payment Service Providers issuing Payment Tokens shall ensure effective and prudent management of the Reserve of Assets. They shall ensure that the creation and destruction of Payment Tokens is matched by a corresponding increase or decrease in the Reserve of Assets and that such increase or decrease is adequately managed to avoid any adverse impacts on the market of the Reserve Assets.

Stabilisation Mechanism

10. Payment Service Providers issuing Payment Tokens shall have and maintain a clear and detailed policy on the

selected stabilisation mechanism. That policy and procedure shall in particular:

10.1 describe the type, allocation and composition of the reference assets the value of which aims at stabilising the value of the Payment Tokens;

10.2 contain a detailed assessment of the risks, including credit risk, counterparty risk, market risk and liquidity risk, resulting from the Reserve of Assets;

10.3 describe the procedure for the creation and destruction of Payment Tokens and the consequence of such creation or destruction on the increase and decrease of the Reserve of Assets;

10.4 provide information on whether the Reserve of Assets is invested, and where part of the Reserve of Assets is invested, describe in detail the investment policy and contain an assessment of how that investment policy can affect the value of the Reserve of Assets; and

10.5 describe the procedure to purchase and redeem Payment Tokens against the Reserve of Assets, and list the persons who are entitled to such redemption.

11. Payment Service Providers issuing Payment Tokens shall ensure an independent audit of the Reserve of Assets on a bi-annual basis as from the receipt of the Central Bank's approval of the White Paper with respect of the Payment Tokens.

Custody

12. Payment Service Providers issuing Payment Tokens shall establish, maintain and implement custody policies, procedures and contractual arrangements for each category of issued Payment Tokens that ensure at all times that:

12.1 the Reserve of Assets is segregated from the Payment Service Provider's own assets;

12.2 the Reserve of Assets is not encumbered or pledged;

12.3 the Reserve of Assets is held in custody in accordance with paragraph (14); and

12.4 the Payment Service Providers have prompt access to the Reserve of Assets to meet any redemption requests from the holders of Payment Token.

13 The assets received in exchange for the Payment Tokens shall be held in custody by no later than (5) Business Days after the issuance of the Payment Tokens by:

13.1 Bank; or

13.2 Payment Service Provider providing Payment Token Custody.

Investment of the Reserve of Assets

14 Payment Service Providers issuing Payment Tokens that invest a portion of the Reserve of Assets shall invest those assets only in highly liquid financial instruments with minimal market and credit risk. The investments shall be capable of being liquidated rapidly with minimal adverse price effect.

15 All profits or losses, including fluctuations in the value of the financial instruments referred to in paragraph (14), and any counterparty or operational risks that result from the investment of the assets shall be borne by Payment Service Providers issuing the Payment Tokens.

Pre-Trade Transparency

16 Payment Service Providers that engage in Facilitating the Exchange of Payment Tokens shall disclose to its Retail Payment Service Users and the public as appropriate, on a continuous basis during normal trading, the following information relating to trading of each accepted Payment Tokens on their platform:

16.1 the current bid, offer prices and volume;

16.2 the depth of trading interest shown at the prices and volumes advertised through their systems for the accepted Payment Tokens; and

16.3 any other information relating to accepted Payment Tokens which would promote transparency relating to trading.

17 Payment Service Providers that engage in Facilitating the Exchange of Payment Tokens shall use appropriate mechanisms to enable pre- trade information to be made available to the public in an easy to access and uninterrupted manner.

Post-Trade Transparency

18 Payment Service Providers that engage in Facilitating the Exchange of Payment Tokens shall disclose the price, volume and time of the Payment Transactions executed in respect of accepted Payment Tokens to the public as close to real-time as is technically possible on a nondiscretionary basis. They shall use adequate mechanisms to enable post-trade information to be made available to the public in an easy to access and uninterrupted manner, at least during business hours.

Article (12) Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations

1. Payment Service Providers must comply with the relevant UAE AML Laws and Regulations and address money laundering and terrorist financing risks through appropriate preventive measures to deter abuse of the sector as a conduit for illicit funds, and detect money laundering and terrorist financing activities and report any suspicious transactions to the Financial Intelligence Department at the Central Bank.

2. Payment Service Providers must have comprehensive and effective internal AML/CFT policies, procedures and controls in place. Payment Service Providers shall be prohibited from invoking banking, professional or contractual secrecy as a pretext for refusing to perform their statutory reporting obligation in regard to suspicious activity.

3. Payment Service Providers must identify, assess, and understand the ML/FT risks to which they are exposed and conduct enterprise-level and business relationship-specific risk assessments. Accordingly, all AML/CFT CDD, monitoring and controls must be risk-based and aligned to the risk assessments.

4. Payment Service Providers shall undertake periodic risk profiling of Retail Payment Service Users and assessment based on the AML/CFT requirements.

5. Payment Service Providers shall assess whether a business relationship presents a higher money laundering and terrorist financing risk and assign a related risk rating. Payment Service Providers shall be prohibited from dealing in any way with shell banks or other shell financial institutions and from establishing or maintaining any business relationship or conducting any Payment Transaction under an anonymous or fictitious name or by pseudonym or number.

6. Payment Service Providers shall ensure that their CDD models are designed to address the specific risks posed by a Retail Payment Service User profile and Payment Instrument features. Payment Service Providers shall be prohibited from establishing or maintaining any business relationship or executing any Payment Transaction in the event that they are unable to complete adequate risk-based CDD measures for any reason.

7. Payment Service Providers providing Retail Payment Services must undertake certain CDD measures concerning Wire Transfers as stipulated in the relevant provisions of the AML Law if Wire Transfer services are provided by Payment Service Providers. Payment Service Providers should introduce appropriate systems for screening, as part of the CDD process, on all parties involved in a transaction against all applicable sanction lists (i.e. the UN sanction lists and the names contained in the 'search notices'/'search and freeze notices' issued by the Central Bank).

8. If Payment Service Providers provide the service of Wire Transfers, they should take freezing action and prohibit conducting transactions with designated persons and entities, as per the obligations set out in the Central Bank's Notice 103/2020 on the Implementation of United Nations Security Council (UNSC) and the UAE Cabinet Resolutions regarding UNSC and Local Lists, as amended from time to time.

9. Payment Service Providers should also be guided by the Financial Action Task Force (FATF) Standards on anti-money laundering and countering the financing of terrorism and proliferation. Payment Service Providers should

incorporate the regular review of ML/FT trends and typologies into their compliance training programmes as well as into their risk identification and assessment procedures.

Article (13) Technology Risk and Information Security

1. Payment Service Providers shall comply with this Article (13) and are encouraged to consult Annex II for the Guidance on the best practices for technology risk and information security.

Technology Risk

2. Payment Service Providers are expected to take into account international best practices and standards when designing and implementing the technology and specific risk management systems and processes.

3. A Payment Service Provider shall establish an effective technology and cyber security risk management framework to ensure the adequacy of IT controls, cyber resilience, the quality and security, including the reliability, robustness, stability and availability, of its computer systems, and the safety and efficiency of the operations of Retail Payment Services. The framework shall be "fit for purpose" and commensurate with the risks associated with the nature, size, complexity and types of business and operations, the technologies adopted and the overall risk management system of the Payment Service Provider. Consideration shall be given to adopting recognized international standards and practices when formulating such risk management framework.

4. A Payment Service Provider's effective technology risk management framework shall comprise proper IT governance, a continuous technology risk management process and implementation of sound IT control practices.

5. A Payment Service Provider shall establish a general framework for management of major technology-related projects, such as in-house software development and acquisition of information systems. This framework shall specify, among other things, the project management methodology to be adopted and applied to these projects.

6. Payment Service Provider shall apply and meet at a minimum the UAE Information Assurance Standards, as may be amended from time to time.

IT Governance

7. A Payment Service Provider shall establish a proper IT governance framework. IT governance shall cover various aspects, including a clear structure of IT functions and the establishment of IT control policies. While there could be different constructs, the major functions shall include an effective IT function, a robust technology risk management function, and an independent technology audit function.

8. The Board, or a committee designated by the Board shall be responsible for ensuring that a sound and robust risk management framework is established and maintained to manage technology risks in a manner that is commensurate with the risks posed by the Payment Service Provider's Retail Payment Activities.

Security Requirements

9. A Payment Service Provider must define clearly its security requirements in the early stage of system development or acquisition as part of business requirements and adequately built during the system development stage.

10. A Payment Service Provider using the Agile methods to accelerate software development must incorporate adequate security practices to ensure the software is not compromised at any stage in its development process.

11. A Payment Service Provider that develops an Application Programming Interface (API) or provides an API shall establish safeguards to manage the development and provision of the APIs to secure the interaction and exchange of data between various software applications.

Network and Infrastructure Management

12. A Payment Service Provider whose monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above shall clearly assign overall responsibility for network management to individuals who are

equipped with expertise to fulfil their duties. Network standards, design, diagrams and operating procedures shall be formally documented, kept up-to-date, communicated to all relevant network staff and reviewed periodically.

13. A Payment Service Provider shall establish a security administration function and a set of formal procedures for administering the allocation of access rights to system resources and application systems, and monitoring the use of system resources to detect any unusual or unauthorized activities.

14. Payment Service Providers shall exercise due care when controlling the use of and access to privileged and emergency IDs. The necessary control procedures include:
    14.1. changing the default password;
    14.2. implement strong password control, with minimum password length and history, password complexity as well as maximum validity period;
    14.3. restricting the number of privileged users;
    14.4. implementing strong controls over remote access by privileged users;
    14.5. granting of authorities that are strictly necessary to privileged and emergency IDs;
    14.6. formal approval by appropriate senior personnel prior to being released for usage;
    14.7. logging, preserving and monitoring of the activities performed by privileged and emergency IDs (e.g. peer reviews of activity logs);
    14.8. prohibiting sharing of privileged accounts;
    14.9. proper safeguard of privileged and emergency IDs and passwords (e.g. kept in a sealed envelope and locked up inside the data center); and
    14.10. changing of privileged and emergency IDs' passwords immediately upon return by the requesters.

Cyber Security Risk

15. Where a Payment Service Provider is heavily reliant on Internet and mobile technologies to deliver the Retail Payment Services it provides, cyber security risks shall be adequately managed through the Payment Service Provider's technology risk management process. The Payment Service Provider shall also commit adequate skilled resources to ensure its capability to identify the risk, protect its critical services against the attack, contain the impact of cyber security incidents and restore the services.

16. A Payment Service Provider shall establish a cyber incident response and management plan to swiftly isolate and neutralize a cyber threat and to resume affected services as soon as possible. The plan shall describe procedures to respond to plausible cyber threat scenarios

17. Payment Service Providers whose monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above shall regularly assess the necessity to perform penetration and cyber-attack simulation testing. Coverage and scope of testing shall be based on the cyber security risk profile, cyber intelligence information available, covering not only networks (both external and internal) and application systems but also social engineering and emerging cyber threats. A Payment Service Provider shall also take appropriate actions to mitigate the issues, threats and vulnerabilities identified in penetration and cyber-attack simulation testing in a timely manner, based on the impact and risk exposure analysis.

Retail Payment Service User Authentication

18. A Payment Service Provider shall select and implement reliable and effective authentication techniques to validate the identity and authority of its Retail Payment Service Users. Multi- factor authentication shall be required for high- risk transactions.

19. End-to-end encryption shall be implemented for the transmission of Retail Payment Service User passwords so that they are not exposed at any intermediate nodes between the Retail Payment Service User mobile application or browser and the system where passwords are verified.

Login Attempts and Session Management

20. A Payment Service Provider shall implement effective controls to limit the number of login or authentication attempts (e.g. wrong password entries), implementing time-out controls and setting time limits for the validity of authentication. If one-time password is used for authentication purpose, a Payment Service Provider shall ensure that the validity period of such passwords is limited to the strict minimum necessary.

21. A Payment Service Provider shall have processes in place ensuring that all Payment Transactions are logged with an appropriate audit trail.

Administration of Retail Payment Service User Accounts

22. Where a Payment Service Provider providing Payment Account Issuance Services allows a Retail Payment Service User to open a Payment Account through an online channel, a reliable method shall be adopted to authenticate the identity of that Retail Payment Service User. In general, the electronic know your customer (i.e. Retail Payment Service User) (eKYC) processes accepted by the Central Bank for Banks is acceptable for the customer verification and validation processes of Payment Account Issuance Services.

23. A Payment Service Provider shall perform adequate identity checks when any Retail Payment Service User requests a change to the Retail Payment Service User's Payment Account information or contact details that are useful for the Retail Payment Service User to receive important information or monitor the activities of the Retail Payment Service User's Payment Accounts.

24. A Payment Service Provider shall implement effective controls such as two-factor authentication, to re-authenticate the Retail Payment Service User before effecting each high-risk transaction. High-risk transactions shall, at least, include:

24.1 Payment Transactions that exceeded the predefined transaction limit(s);

24.2 Change of personal contact details; and

24.3 Unless it is not practicable to implement, Payment Transactions that exceeded the aggregate rolling limit(s) (i.e. total value of Payment Transactions over a period of time).

Business Continuity

25. A Payment Service Provider shall have in place an adequate business continuity management program to ensure continuation, timely recovery, or in extreme situations orderly scale- down of critical operations in the event of major disruptions caused by different contingent scenarios. An adequate business continuity management program comprises business impact analysis, recovery strategies, a business continuity plan and alternative sites for business and IT recovery.

26. A Payment Service Provider shall put in place a set of recovery strategies to ensure that all critical business functions identified in a business impact analysis can be recovered in accordance with the predefined recovery timeframe. These recovery strategies shall be clearly documented, thoroughly tested and regularly reviewed to ensure achievement of recovery targets.

27. A Payment Service Provider shall put in place effective measures to ensure that all business records, in particular Retail Payment Service User records, can be timely restored in case they are lost, damaged, or destroyed. A Payment Service Provider shall also allow Retail Payment Service Users to access their own records in a timely manner. A Payment Service Provider shall notify Retail Payment Service Users of any loss in their records through an operational failure or through theft, and make reasonable effort to ensure that personal records so lost are not used wrongfully.

28. A Payment Service Provider shall develop a business continuity plan based on the business impact analysis and related recovery strategies. A business continuity plan shall comprise, at a minimum:

28.1. detailed recovery procedures to ensure full accomplishment of the service recovery strategies;

28.2. escalation procedures and crisis management protocol (e.g. set up of a command center, timely reporting to the Central Bank, etc.) in case of severe or prolonged service disruptions;

28.3. proactive communication strategies (e.g. Retail Payment Service User notification, media response, etc.);

28.4. updated contact details of key personnel involved in the business continuity plan; and

28.5. assignment of primary and alternate personnel responsible for recovery of critical systems.

29. A Payment Service Provider shall conduct testing of its business continuity plan at least annually. Its Management, primary and alternate relevant personnel shall participate in the annual testing to familiarize themselves with their recovery responsibilities.

30. A Payment Service Provider shall review all business continuity planning-related risks and assumptions for relevancy and appropriateness as part of the annual planning of testing. Formal testing documentation, including a test plan, scenarios, procedures and results, shall be produced. A post mortem review report shall be prepared for formal sign-off by Management

Alternate Sites for Business and IT Recovery

31. A Payment Service Provider shall examine the extent to which key business functions are concentrated in the same or adjacent locations and the proximity of the alternate sites to primary sites. Alternate sites shall be sufficiently distanced to avoid any shared risk and being affected by the same disaster.

32. A Payment Service Provider's alternate site shall be readily accessible, installed with appropriate facilities and available for occupancy within the time requirement specified in its business continuity plan. Appropriate physical access controls shall be implemented. If certain recovery staff are required to work from home in the event of a disaster, adequate computer systems and communication facilities shall be made available in advance.

33. Alternate sites for IT recovery shall have sufficient technical equipment, including communication facilities, of an appropriate standard and capacity to meet recovery requirements.

34. A Payment Service Provider shall avoid placing excessive reliance on external vendors in providing business continuity management support, including the provision of the disaster recovery site and back-up equipment and facilities. A Payment Service Provider shall satisfy itself that each vendor has the capacity to provide the services when needed, and that the contractual responsibilities of the vendors, including the lead-time to provide necessary emergency services, types of support and capacity, are clearly specified.

35. Where a Payment Service Provider is reliant on shared computing services provided by external providers, such as cloud computing, to support its disaster recovery, it shall manage the risk associated with these services.

Reputation Risk Management

36. A Payment Service Provider shall establish and implement an effective process for managing reputational risk that is appropriate for the size and complexity of its operations.

Article (14): Obligations Towards Retail Payment Service Users

1. Payment Service Providers must be operated prudently and with competence in a manner that will not adversely affect the interests of the Retail Payment Service Users or potential Retail Payment Service Users. In addition, they must also observe and comply with the relevant regulatory requirements and standards on consumer protection of the Central Bank. For the avoidance of doubt, in case of discrepancies between this Regulation and the Central Bank's requirements and standards on consumer protection, the respective provisions of this Regulation shall prevail.

Safeguarding of Funds In-Transit

2. At no time shall Payment Service Providers hold funds of Retail Payment Service Users unless these are funds in transit.

3. Payment Service Providers that settle Payment Transactions within twenty four (24) hours shall segregate Retail Payment Service Users' funds in the following ways:

3.1. funds shall not be commingled at any time with the funds of any Person other than the Retail Payment Service Users on whose behalf the funds are held; and/or

3.2. funds shall be insulated in the interest of the Retail Payment Service Users against the claims of other creditors of the Payment Service Provider, in particular in the event of insolvency.

4. Payment Service Providers that settle Payment Transactions after twenty-four (24) hours shall segregate Retail Payment Service Users' funds in the following ways:

4.1. open a separate escrow account with a Bank and restrict any operations and transactions on this account save for the transfer of the deposited Retail Payment Service Users' funds to the end beneficiary; and/or

4.2. funds shall be covered by an insurance policy or by a bank guarantee from a regulated insurance company or Bank which does not belong to the same Group as the Payment Service Provider.

4.3. While Banks, acting as Retail Payment Service Provider, are not required to establish a separate escrow account, an insurance policy or a bank guarantee to safeguard Retail Payment Service Users' funds, a separate bank account under the name of the concerned Retail Payment Service Users must be set up for protecting the funds.

Transparency of Contractual Terms

5. Payment Service Providers shall provide the terms and conditions governing their contractual relationship with:

5.1. each new Retail Payment Service User, sufficiently in advance of entering into the contractual relationship as to allow the Retail Payment Service User to make an informed decision; and

5.2. each existing Retail Payment Service User, at their request in writing and delivered as per the Retail Payment Service User's preference, including through an e-mail, mobile application or any other electronic manner.

6. The terms and conditions referred to in paragraph (5) shall be written in a clear, plain and understandable language, in a manner that is not misleading and shall be provided to the Retail Payment Service User in both Arabic and English, as may be requested by the Retail Payment Service User.

7. Any changes to the terms and conditions referred to in paragraph (5) shall be communicated to the Retail Payment Service User by the Payment Service Provider sufficiently in advance and at least 30 calendar days prior to any such change becoming effective.

8. A Retail Payment Service User shall be entitled to terminate its contractual relationship with a Payment Service Provider at no charge where it does not agree with the revised terms and conditions referred to in paragraph (7).

Single Retail Payment Service Agreements

9. For transactions that are to be concluded under a Single Retail Payment Service Agreement, Payment Service Providers shall provide Retail Payment Service Users with the following information before the entry into a contractual
relationship:

9.1. schedule of fees, charges and commissions, including conversion rates and withdrawal charges, where applicable;

9.2. contact details of the Payment Service Provider, including legal name and registered address, including the address of the agent or branch, where applicable;

9.3. the form and procedure for giving consent to the initiation of a Payment Order or execution of a Payment Transaction and for the withdrawal of consent;

9.4. the communication channel between the Payment Service Provider and the Retail Payment Service User;

9.5. the manner in safeguarding of funds as per Article 14(3) and (4) and Reserve of Assets as per Article 11(9);

9.6. the manner and timeline for notification by the Retail Payment Service User to the Payment Service Provider in case of Unauthorized or incorrectly initiated or executed Payment Transaction;

9.7. information on Payment Service Provider's and Retail Payment Service User's liability for Unauthorized Payment Transactions;

9.8. the service level for the provision of the Retail Payment Service;

9.9. information on the Payment Service Provider's complaint procedure; and

9.10. the Payment Service Provider's procedure for reporting of Unauthorized Payment Transactions.

10. The information required in paragraph (9) shall be provided immediately after the execution of the Payment Transaction where it is concluded at a Payment Service User's request using a Means of Distance Communication which does not allow for the provision of such information before the entry into a contractual relationship.

Framework Agreements

11. For transactions that are concluded under a Framework Agreement, Payment Service Providers shall provide to Retail Payment Service Users the following information before the Retail Payment Service User consents to the

entry into a Payment Transaction as well as at any other time the Retail Payment Service User requests this information, and within (5) Business Days of such request:

11.1. schedule of fees, charges and commissions, including conversion rates and withdrawal charges, where applicable;

11.2. contact details of the Payment Service Provider, including legal name and registered address, including address of the agent or branch, where applicable;

11.3. the form and procedure for giving consent to the initiation of a Payment Order or execution of a Payment Transaction and for the withdrawal of consent;

11.4. the communication channel between the Payment Service Provider and the Retail Payment Service User;

11.5. the manner in safeguarding of funds as per Article 14(3) and (4) and Reserve of Assets as per Article 11(9);

11.6. the manner and timeline for notification by the Retail Payment Service User to the Payment Service Provider in case of Unauthorized or incorrectly initiated or executed Payment Transaction;

11.7. information on Payment Service Provider's and Retail Payment Service User's liability for Unauthorized Payment Transactions;

11.8. information relating to terms under which a Payment Service User may be deemed to have accepted changes to the terms and conditions, the duration of the contract and the rights of the parties to terminate the Framework Agreement;

11.9. the service level for the execution of the Retail Payment Service;

11.10. information on the Payment Service Provider's complaint procedure; and

11.11. the Payment Service Provider's procedure for reporting of Unauthorized Payment Transactions.

12. The information required in paragraph (11) shall be provided immediately after the execution of the Payment Transaction where it is concluded at a Payment Service User's request using a Means of Distance Communication which does not allow for the provision of such information before the entry into a contractual relationship.

13. Payment Service Providers shall provide Retail Payment Service Users with a written statement of the Payment Transactions under a Framework Agreement at least once per month free of charge, including details of the amounts, fees, charges and commissions, the dates and times of execution and the reference numbers for each Payment Transaction.

Information Requirements

14. Immediately after the receipt of an order for a Payment Transaction, the Payment Service Provider of the Payer shall provide a receipt for Retail Payment Service Users with:

14.1. confirmation of the successful or unsuccessful initiation and execution of the Payment Transaction;

14.2. acknowledgement and reference number to track the status of the Payment Transaction, including:

14.2.1. the date and amount of the Payment Transaction; and

14.2.2. information relating to the Payee;

14.3. the amount of the Payment Transaction, any related fees or charges, including the actual currency and conversion rates used, and withdrawal charges, where applicable; and

14.4. the date on which the Payment Service Provider received the Payment Order.

15. The Payee's Payment Service Provider shall, immediately after the execution of the Payment Transaction, provide to the Payee with a statement with the following information:

15.1. reference enabling the Payee to identify the Payment Transaction and, where appropriate, the Payer and any information transferred with the Payment Transaction;

15.2. the amount of the Payment Transaction in the currency in which the funds are to be dispersed disbursed to the Payee;

15.3. the amount of any fees or charges for the Payment Transaction payable by the Payee;

15.4. where applicable, the currency exchange rate used in the Payment Transaction by the Payee's Payment Service Provider; and

15.5. the date on which the amount of a Payment Transaction is credited to a Payee's Payment Account.

16. The Payer's Payment Service Provider shall ensure that Payment Orders are accompanied by the necessary information so that they can be processed accurately and completely, and also, be easily identified, verified, reviewed, audited and for any subsequent investigation if needed.

17. The Payee's Payment Service Provider shall implement procedures to detect when any necessary information is missing or inaccurate for a Payment Transaction.

Protection of Payment and Personal Data

18. Payment Service Providers shall have in place and maintain adequate policies and procedures to protect:

18.1. Payment Data and identify, prevent and resolve any data security breaches; and

18.2. Personal Data.

19. Payment Service Providers may disclose Payment and Personal Data to:

19.1. a third party where the disclosure is made with the prior written consent of the Retail Payment Service User or is required pursuant to applicable laws;

19.2. to the Central Bank;

19.3. other regulatory authorities upon request/following prior approval of the Central Bank;

19.4. a court of law; and

19.5. other government bodies who have lawfully authorized rights of access.

20. In addition to the envisaged in paragraph (19), Payment Service Providers may also disclose Personal Data to its corresponding Data Subject.

21. Payment Service Providers shall have in place and maintain Payment and Personal Data protection controls.

22. Personal and Payment Data shall be stored and maintained in the State. Payment Service Providers must also establish a safe and secure backup of all Personal and Payment Data in a separate location for the required period of retention of (5) years.

23. Payment Service Providers shall comply with applicable regulatory requirements and standards on data protection. They shall control, process and retain only Personal Data that is necessary for the provision of Retail Payment Services and upon obtaining the explicit consent of the Retail Payment Service User.

Liability for Unauthorized Payment Transactions and Refunds

24. Payment Service Providers shall be fully liable for any fraudulent or Unauthorized Payment Transaction, whether before or after the Payer informs the Payment Service Provider of any potential or suspected fraud, except where there is evidence that:

24.1. the Payer acts fraudulently; or

24.2. the Payer acted with gross negligence and did not take reasonable steps to keep its personalized security credentials safe.

Refunds

25. The Payment Service Provider shall refund the amount of the Unauthorized Payment Transaction to the Payer and, where applicable, restore the debited Payment Account to the state it would have been in had the Unauthorized Payment Transaction not taken place.

26. The Payment Service Provider shall provide a refund under paragraph (25) as soon as practicable and in any event no later than the end of the Business Day following the day on which it becomes aware of the Unauthorized Payment Transaction.

27. Paragraphs (25), (26) and (30) do not apply where the Payment Service Provider has reasonable grounds to suspect fraudulent behavior by the Retail Payment Service User and notifies the Central Bank of those grounds in writing.

28. When crediting a Payment Account under paragraph (30), a Payment Service Provider shall ensure that the date on which the amount of a Payment Transaction is credited to a Payee's Payment Account is no later than the date on which the amount of the Unauthorized Payment Transaction was debited.

29. Where an Unauthorized Payment Transaction was initiated through a Payment Initiation Service Provider, the Payment Service Provider providing Payment Account Issuance Services shall comply with paragraph (30). In addition, if the Payment Initiation Service Provider is liable for the Unauthorized Payment Transaction, it shall, on the request of the Payment Service Provider providing Payment Account Issuing Services, compensate the Payment Service Provider providing Payment Account Issuing Services immediately for the losses incurred or sums paid as a result of complying with paragraph (30), including the amount of the Unauthorized Payment Transaction.

30. Other than in relation to the circumstances contemplated in paragraphs (25) to (29), on conclusion of an investigation by a Payment Service Provider into an error or Complaint, a Payment Service Provider shall pay any refund or monetary compensation due to a customer within (7) calendar days of such conclusion or instruction. In case of a delay in payment of any refund or compensation, the Payment Service Provider shall update the customer with the expected time for crediting the amount due, along with a justification for the delay.

Article (15): Use of Agents and Branches

1. Where a Payment Service Provider intends to provide Retail Payment Services through an Agent or branch, it must conduct an assessment of such arrangement and provide a report on an annual basis to the Central Bank of the following:

1.1. name and address of the Agent or branch;

1.2. assessment of the adequacy of the internal control mechanisms that will be used by the Agent in order to comply with AML/CTF requirements;

1.3. assessment of the Persons responsible for the Management of the Agent or branch, and evidence that they fulfil the fit and proper requirements specified by the Central Bank; and

1.4. the scope of Retail Payment Services for which the Agent or branch is mandated.

2. Payment Service Providers shall contractually ensure that Agents acting on their behalf disclose this fact to the Retail Payment Service Users.
3. Payment Service Providers shall immediately notify the Central Bank of any change regarding the use of Agents or branches.

Article (16): Outsourcing

1. Payment Service Providers outsourcing services and processes to service providers, Agents or Group entities shall be obliged to contractually ensure that such third parties comply with the requirements of this Regulation, Level 2 Acts and other relevant laws.
2. The outsourcing under paragraph (1) shall be subject to the prior approval of the Central Bank. Furthermore, Payment Service Providers shall provide details on all outsourcing under paragraph (1) in a report on an annual basis to the Central Bank.
3. Payment Service Providers shall remain fully liable for any acts of any Agent, branch or service provider to which a Retail Payment Service has been outsourced.
4. Payment Service Providers shall be responsible for ensuring and maintaining appropriate training and qualifications of their Agents.

Article (17): Contractual Arrangements

Access to Payment Accounts

1. Payment Service Providers providing Payment Account Issuance Services and/or Banks may agree to contract with Payment Service Providers providing Payment Initiation and Payment Account Information Services for the provision of access, direct or indirect, to the Payment Accounts held with them in order to allow such Payment Service Providers to provide Payment Initiation and Payment Account Information Services in an unhindered and efficient manner.
2. The contractual arrangements under paragraph (1) shall:
    2.1. have a sound legal basis and be legally enforceable;
    2.2. clearly describe the rights and obligations of the counterparties;
    2.3. clearly define the allocation of liability between the counterparties, including in cases of fraud, unauthorized access or Data Breach, in a manner that each counterparty takes responsibility for the respective parts of the Payment Transaction under its control;
    2.4. specify the reasons for denying access to Payment Accounts related to unauthorized or fraudulent access by Payment Service Providers providing Payment Initiation and Payment Account Information Services; and
    2.5. explicitly oblige the counterparties to comply with Article (13) on Technology Risk and Information Security.
3. The choice of Payment Service Providers providing Payment Initiation and Payment Account Information Services shall be at the sole discretion of the Payment Service Providers providing Payment Account Issuance Services and/or Banks.
4. Payment Service Providers providing Payment Initiation and Payment Account Information Services shall:
    4.1. provide services only where based on the Retail Payment Service User's explicit consent;
    4.2. ensure that the personalized security credentials of the Retail Payment Service User are not, with the exception of the Retail Payment Service User and the issuer of the personalized security credentials, accessible to other parties and that they are transmitted through safe and efficient channels;
    4.3. not request or store Sensitive Payment Data of the Retail Payment Service User;

4.4. not use, access or store any data for purposes other than for the provision of the Payment Initiation or Payment Account Information Services, as explicitly requested by the Retail Payment Service User; and

4.5. comply with the requirements of Article (13) on Technology Risk and Information Security where the Payer initiates an electronic Payment Transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

5. In addition to the requirements set out in paragraph (4), Payment Service Providers providing Payment Account Information Services shall access only the information from designated Payment Accounts and associated Payment Transactions.

6. In addition to the requirements set out in paragraph (4), Payment Service Providers providing Payment Initiation Services shall not modify the amount, the Payee or any other feature of the Payment Transaction.

Article (18): Card Schemes

Card Scheme License

1. Card Schemes operating within the State shall obtain a License by the Central Bank prior to commencing operations.
2. Applicants shall be subject to the procedure envisaged in the Central Bank's Licensing Guidelines.
3. The Central Bank shall determine whether to grant or refuse to grant a License to a Card Scheme Applicant and indicate this in writing to the Applicant within (90) calendar days from the receipt of the full set of documents and information requested under the Application.
4. The Central Bank may grant a License under paragraph (1) with or without conditions or restrictions attached to it, or refuse to grant a License at its discretion.
5. The Central Bank shall notify the Card Scheme of the decision taken under paragraph (3). In case of a refusal to grant a License, the Central Bank shall indicate the reasons for such refusal.
6. The Central Bank reserves the sole right to issue Card Issuer (Bank) Identification Numbers (BIN) in accordance with ISO/IEC 7812, as may be amended or supplemented from time to time.

License Conditions

7. The Central Bank shall grant a License to a Card Scheme under this Article (18) upon the fulfilment of the following conditions:

7.1. the Central Bank has been provided with all necessary documents and information as it may request, in the form and within the timeframe specified by it, to allow it to assess the adequacy, efficiency and soundness of a Card Scheme, including:

7.1.1. the business model and business strategy;

7.1.2. the corporate governance structure;

7.1.3. the Management contact details;

7.1.4. the ownership and Group structure;

7.1.5. the financial and operational resources; and

7.1.6. the description of key risks, including conduct of business and money laundering and terrorist financing risks;

7.2. the Management of the Card Scheme fulfil the fit and proper requirements specified by the Central Bank, including that each member of Management:

7.2.1. possesses the necessary knowledge, skills, and experience;

7.2.2. has a record of integrity and good repute;

7.2.3. has sufficient time to fully discharge the responsibilities under this Regulation and Level 2 Acts; and

7.2.4. has a record of financial soundness.

Reporting Requirements

8. A Card Scheme that has been granted a License shall:

8.1. report to the Central Bank the information contained in Annex III on a quarterly basis;

8.2. provide additional information or become subject to more frequent reporting, as deemed necessary by the Central Bank; and

8.3. report immediately any changes that affect or are likely to affect its business model or financial viability, or which may otherwise be deemed to be material in nature such as significant increase or decrease in transaction volumes.

Ongoing Requirements

Governance

9. The Board and Management of a Card Scheme shall be responsible for ensuring that a licensed Card Scheme has an internal control framework that is adequate to establish a properly controlled operating environment for the conduct of its business, taking into account its risk profile.

10. Management shall be responsible for developing an internal control framework that identifies, measures, monitors and controls all risks faced by the Card Scheme.

11. Licensed Card Schemes shall have organizational structures that incorporate a “three lines of defense” approach comprising the business lines, the support and control functions and an independent internal audit function.

Compliance Function

12. The Board shall be responsible for ensuring that a Card Scheme has an independent, permanent and effective compliance function to monitor and report on observance of all applicable laws, regulations and standards and on adherence by staff and members of the Board to legal requirements, proper codes of conduct and policy on conflicts of interest.

13. The Card Payment Scheme shall have a Board- approved compliance policy that is communicated to all staff specifying the purpose, standing and authority of the compliance function within the Card Scheme.

14. Card Schemes shall establish appropriate policies, procedures and controls pertaining to the internal reporting by their Management and staff of suspicious transactions, including the provision of the necessary records and data, to the designated Anti-Money Laundering and Combating the Financing of Terrorism compliance officer for further analysis and reporting decisions. Card Schemes shall report transactions to the competent authority when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime.

Internal Audit Function

15. The Board shall be responsible for ensuring that the Card Scheme has an independent, permanent and effective internal audit function commensurate with the size, nature of operations and complexity of its organization.

16. The internal audit function shall provide independent assurance to the Board and Management on the quality and

effectiveness of the Card Scheme's internal controls, risk management, compliance, corporate governance, and the systems and processes created by the business units, support and control functions.

17. The Card Scheme shall have an internal audit charter approved by the Board audit committee that articulates the purpose, standing and authority of the internal audit function within the Card Scheme.

Risk Management

18. Card Schemes shall have an adequately resourced risk management function headed by a chief risk officer or equivalent. The function shall be independent of the management and decision-making of the Card Scheme's risk-taking functions. The risk management function shall include policies, procedures, systems and controls for monitoring and reporting risks, and to ensure that risk exposures are aligned with the entity's strategy and business plan.

Risk Strategy

19. Card Schemes shall have a clearly defined business strategy, risk appetite and defined corporate culture that has been approved by the Board and reviewed at least annually. Management shall ensure full compliance of this articulated strategy across all business lines and the Board will be ultimately responsible for such compliance.

Information Security

20. A Card Scheme shall apply and meet at a minimum the Payment Card Industry Data Security Standard ('PCI DSS') and UAE Information Assurance Standards, as may be amended from time to time.

21. A compliance report regarding the Card Scheme's adherence to the standards referred to in paragraph (20) shall be presented to the Board at least annually as well as transmitted to the Central Bank.

22. In the case of a Data Breach, the Card Scheme shall notify the Central Bank without undue delay and not later than (72) hours after having become aware of such Data Breach.

Disaster Recovery and Business Continuity Management

23. Card Schemes shall have disaster recovery and business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption. Such plans must be commensurate with the risk profile, nature, size and complexity of the Card Scheme's business and structure and take into account different scenarios to which the Card Scheme may be vulnerable.

24. Disaster recovery and business continuity plans shall ensure that critical business functions of the Card Scheme can be maintained and recovered in a timely manner to minimize the financial, legal, regulatory, reputational and other risks that may arise from a disruption.

25. The Board shall ensure there is a periodic independent review of the Card Scheme's disaster recovery and business continuity plans to ensure adequacy and consistency with current operations, risks and threats, recovery levels and priorities.

Risk Assessment

26. Card Schemes shall regularly assess risks through the identification of new risks, measurement of known risks and prioritization of risks through thorough understanding of the business and the market.

Risk Mitigation

27. Card Schemes shall mitigate risks through the implementation of:

    27.1. risk mitigation programs and technologies;
    27.2. the effective management of risk principles; operation with risk management in mind; and

27.3. outsourcing of risk functions that cannot be performed in-house.

Monitoring

28. Card Schemes shall perform regular monitoring of all risks and mitigation programs on at least an annual basis to ensure the robustness of the risk management procedures and programs. Continuous monitoring reports, including dashboards, shall be presented to the Management and the Board to ensure that all levels of management are aware of the current risk situation, including potential fraud, in the Card Scheme.

Assurance

29. Card Schemes shall give assurance to all stakeholders through external and internal audits.

Winding Down

30. Where a Card Scheme intends to terminate its operation in the State, it shall obtain an approval from the Central Bank to this effect.

31. A Card Scheme shall notify the Central Bank in advance of (3) months from the intended termination of its operations, and provide an orderly wind-down plan.

Supervisory Examinations

32. The Central Bank may conduct periodic examinations of the operation of Card Schemes to ensure their financial soundness and compliance with the requirements of this Regulation and Level 2 Acts.
33. Card Schemes shall provide the Central Bank with full and unrestricted access to their accounts, records and documents, and shall supply such information and facilities as may be required to conduct the examination referred to in paragraph (32).

Fees and Charges

34. The Central Bank has the right to receive information on any fees and charges of Card Schemes and regulate such fees and charges as it considers appropriate.

35. The Central Bank may publicly disclose the fees and charges of Card Schemes referred to in paragraph (34).

Article (19): Access to the Wages Protection System

Eligibility and Conditions

1. Payment Service Providers are eligible to apply to the Central Bank to participate in and, be given access to the Wages Protection System. They shall be given access to the Wages Protection System subject to an approval granted by the Central Bank.
2. To allow wages to be credited to an account that can store and maintain the funds, Payment Service Providers may engage with an SVF scheme or a Bank for the provision of such account. Payment Service Providers that apply for participation in and access to the Wages Protection System shall demonstrate, among other things, that they have stringent security measures put in place so as to minimize the risks to the Wages Protection System.
3. Upon being given access to the Wages Protection System, Payment Service Providers shall be entitled to open WPS Payment Accounts.
4. The requirements in this Article (19) are without prejudice to other requirements of this Regulation to which Payment Service Providers are subject.

Obligations

5. Payment Service Providers that have been given access to the Wages Protection System under paragraph (1) shall:

5.1. organize marketing campaigns targeting the unbanked and underbanked segments with the objective of educating WPS Payment Account Holders on the benefits and risks associated with the services provided by the Payment Service Providers;

5.2. conduct workshops with the objective of raising awareness of Employers on the salary information file (SIF) format to be submitted, penalties and related procedures and regulatory requirements;

5.3. ensure that they provide WPS Payment Account Holders with a transaction statement in a timely manner;

5.4. execute the payments to WPS Payment Account Holders in a timely manner and acknowledge such execution in accordance with the WPS Rulebook;

5.5. not hold WPS Payment Account Holders liable for any fraudulent or Unauthorized Payment Transactions, and shall guarantee the full amount of funds; and

5.6. provide a dedicated Retail Payment Service User service and complaints team for WPS Payment Account Holders that are separate from the equivalent teams servicing other Retail Payment Services that may be provided by the Payment Service Providers.

6. Payment Service Providers that fail to comply with the requirements of paragraph (5.4) shall be subject to the penalties specified in the WPS Rulebook.

7. The Central Bank may request from the Payment Service Providers that have been given access to the Wages Protection System under paragraph (1) to:

7.1. prepare and provide quarterly reports on the average Payment Transactions value per WPS Payment Account Holder; and

7.2. prepare and provide quarterly reports on the number of WPS Payment Account Holders being serviced.

Article (20): Enforcement and sanctions

Violation of any provision of this Regulation or committing any of the violations provided for under the Central Bank Law may subject the Payment Service Provider or Card Scheme to administrative and financial sanctions and penalties as deemed appropriate by the Central Bank.

Article (21): Transition Period

A one-year transitional period will commence on the date this Regulation comes into force. The Central Bank may order the cessation of provision of the Retail Payment Services or the operations of the Card Scheme if the Payment Service Provider or the Card Scheme concerned has not obtained the relevant License from the Central Bank before the end of the transition period. The Central Bank may extend the transition period for the Applicant at its own discretion.

Article (22): Interpretation of Regulation

The Regulatory Development Division of the Central Bank shall be the reference for interpretation of the provisions of this Regulation.

Article (23): Publication & application

1. This Regulation shall be published in the Official Gazette in both Arabic and English and shall come into effect one month from the date of publication. In case of any discrepancy between the Arabic and the English, the Arabic version will prevail.

Khaled Mohamed Balama

Governor of the Central Bank of the United Arab Emirates

Annex I: Retail Payment Services

1. Payment Account Issuance Service
2. Payment Instrument Issuance Service
3. Merchant Acquiring Service
4. Payment Aggregation Service
5. Domestic Fund Transfer Service
6. Cross-border Fund Transfer Service
7. Payment Token Service
8. Payment Initiation Service
9. Payment Account Information Service

Annex II: Guidance on the Best Practices for Technology Risk and Information Security

The following best practices will enable Payment Service Providers to operate adaptive and responsive cyber resilience processes. Payment Service Providers are encouraged to discuss and consider their application to improve their technology risk, information security and cyber resilience preparedness.

Technology Risk

An incident management framework with sufficient management oversight to ensure effective incident response and management capability to deal with significant incidents properly should include:

(i) timely reporting to the Central Bank of any confirmed technology-related fraud cases or major security breaches, including cyber- attacks, cases of prolonged disruption of service and systemic incidents where Retail Payment Service Users suffer from monetary loss or Retail Payment Service Users' interests are being affected (e.g. data leakage); and

(ii) a communication strategy to address the concerns any stakeholders may have arising from the incidents and restore the reputational damage that the incidents may cause.

Change Management

Payment Service Providers whose monthly average value of Payment Transactions amounts to (10) million Dirham or above are encouraged to:

(i) develop a formal change management process to ensure the integrity and reliability of the production environment and that the changes to application systems, system software (e.g. operating systems and utilities), hardware, network systems and other IT facilities and equipment, are proper and do not have any undesirable impact on the production environment. Formal procedures for managing emergency changes (including the record keeping and endorsement arrangement) should also be established to enable unforeseen problems to be addressed in a timely and controlled manner; and

(ii) adequately and accurately document control procedures and baseline security requirements, including all configurations and settings of operating systems, system software, databases, servers and network devices. They are also expected to perform periodic reviews on the compliance of the security settings with the baseline standards.

Project Life Cycle

A full project life cycle methodology governing the process of developing, implementing and maintaining major computer should be established.

Where a software package is acquired from vendors, a formal software package acquisition process should be established to manage risks associated with acquisitions, such as breach of software license agreement or patent infringement.

Quality assurance reviews of major technology- related projects by an independent party, with the assistance of the legal and compliance functions should be conducted.

IT Governance
A set of IT control policies that fits the business model and technology applications should be implemented. The IT control policies which establish the ground rules for IT controls should be formally approved by Management and properly implemented among IT functions and business units. Processes used to verify compliance with IT control policies and the process for seeking appropriate approval by Management for dispensation from IT control policies are also be clearly specified, and consequences associated with any failure to adhere to these processes should be effected.

Security Requirements
Guidelines and standards for software development are adopted with reference to industry generally accepted practices on secure development. Source code reviews (e.g. peer review and automated analysis review), which could be risk-based, as part of a software quality assurance process should be conducted.

Formal testing and acceptance processes should be conducted to ensure that only properly tested and approved systems are promoted to the production environment. The scope of tests covers business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

Segregated environments for development, testing and production purposes should be maintained. System testing and user acceptance testing (UAT) should be properly carried out in the testing environment. Production data should not be used in development or acceptance testing unless the data has been desensitized and prior approval from the information owner has been obtained.

A segregation of duties among IT teams should be introduced. Developers should not be permitted to access to production libraries and promote programming code into the production environment. If automated tools are used for the promotion of programming code, adequate monitoring, reviews and checks by independent teams should be done. Vendor accesses to the UAT environment, if necessary, should be closely monitored.

An inventory of end-user developed applications and where necessary, control practices and responsibilities with respect to end-user computing to cover areas such as ownership, development standards, data security, documentation, data/file storage and backup, system recovery, audit responsibilities and training should be established.
A problem management process to identify, classify, prioritize and address all IT problems in a timely manner should be established. It should perform a trend analysis of past incidents regularly to facilitate the identification and prevention of similar problems.

Network and Infrastructure Management
Network security devices such as firewalls at critical junctures of its IT infrastructure should be installed to secure the connection to untrusted external networks, such as the Internet and connections with third parties.

Where mobile devices are provided to employees, policies and procedures covering, among others, requisition, authentication, hardening, encryption, data backup and retention should be established.

Adequate measures to maintain appropriate segregation of databases for different purposes to prevent unauthorized or unintended access or retrieval and robust access controls should be enforced to ensure the confidentiality and integrity of the databases. In respect of any Personal Data of Retail Payment Service Users, including Merchants, the relevant data protection laws as well as any relevant codes of practice, guidelines or best practice issued by the Central Bank or any other relevant authorities should be assessed from time to time.

Access to the information and application systems should be restricted by an adequate authentication mechanism associated with access control rules. A role-based access control framework should be adopted and access rights should be granted on a need-to-have basis.

Cyber Security Risk
The trends in cyber threats should be considered, including subscribing to quality cyber threat intelligence services, which are relevant to the provision of Retail Payment Services to enhance ability to precisely respond to new type of threats in a timely manner. The Payment Service Provider may also seek opportunities to collaborate with other organizations to share and gather cyber threat intelligence with the aim of facilitating the Retail Payment Services industry to better prepare and manage cyber security risks.

Monitoring or surveillance systems to ensure being alerted to any suspicious or malicious system activities such as multiple sessions of same account from different geographic locations should be carried out. Real-time monitoring of cyber events for critical systems should be performed to facilitate the prompt detection of anomalous activities.

Close attention should be paid to evolving risks related to accessing critical IT infrastructure and appropriate measures are accordingly taken.

Payment Acceptance Devices

Retail Payment Service User devices should be assumed to be exposed to security vulnerabilities and appropriate measures when designing, developing and maintaining Retail Payment Services should be taken. Security measures to guard against different compromising situations, including unauthorized device access, malware or virus attack, compromised or unsecure status of mobile device and unauthorized
mobile applications should be taken.

Where Merchants use mobile devices to accept a Payment Service Provider's Retail Payment Services, additional security measures should be implemented to safeguard the mobile payment acceptance solution, including the detection of abnormal activities and logging them in reports, and the provision of Merchant identification for Retail Payment Service Users to validate identity.

Retail Payment Service User Authentication

Retail Payment Service User authentication based on a multi-factor authentication by combining any two or more of the following three factors is adopted:

(i) verification information specified by Retail Payment Service User knows (e.g. user IDs and passwords);

(ii) verification information a Retail Payment Service User has provided or possesses (e.g. one-time passwords generated by a security token or a Payment Service Provider's security systems); and

(iii) physical verification information belonging to a Retail Payment Service User (e.g. retina, fingerprint or voice recognition).

If a password (including a personal identification number) is used as one factor of authentication, adequate controls related to the strength of the password (e.g. minimum password length) should be put in place.

Login attempts and session management

Robust log files allowing retrieval of historical data including a full audit trail of additions, modifications or deletions of transactions are provided. Access to such tools, including privileged responsibilities, should only be available to authorized personnel and is appropriately logged.

Retail Payment Service Users should be provided with channels to check their Past Payment Transactions.

Fraud Detection Systems

Payment Transaction monitoring mechanisms designed to prevent, detect and block fraudulent Payment Transactions should be operated by Payment Service Providers providing Payment Token Services and Payment Service Providers whose monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above. Suspicious or high-risk transactions are subject to a specific screening, filtration and evaluation procedure.

Annex III: Information to be reported by Card Schemes in English and Arabic

I. ATM data:

Field Name	Max Size	Type	Field Details
Primary Account Number (PAN)	16-19	Numeric	PAN is a series of digits used to identify a Retail Payment Service User account or relationship
Transaction Code	2	Numeric	Transaction Code - 31 (Balance Enquiry), 01 (Cash Withdrawal).
Transaction Amount	12	Numeric	Transaction amount gives the value of the funds requested by the cardholder in the local currency of the acquirer or source location of the transaction.
Transaction Currency Code	3	Alphabet (or) Numeric	Identifies the local currency of the acquirer or source location of the transaction. See ISO 4217.
Transmission Date and Time	10	Numeric	MM/DD/hh/mm/ss format The date used is the current calendar day in Greenwich Mean Time (GMT) that the transaction occurred (not Business Day)
Systems Trace Audit Number	6	Numeric	Contains a number assigned by the transaction acquirer to identify uniquely a transaction. The trace number remains unchanged for all messages throughout the life of the transaction.
Merchant's Type	4	Numeric	Contains the classification of the merchant's type (ATM/web/etc) of business product or service.
Acquiring Institution Country Code	3	Numeric	Contains the code of the country where the acquiring institution is located (see ISO 3166)
Point of Service Entry Mode	3	Numeric	Contains two numeric to indicate the method by which the primary account number was entered into the system and one numeric to indicate the PIN entry capabilities.
Acquiring Institution Identification Component	11	Numeric	Contains a code identifying the acquiring institution (e.g. merchant bank) or its agent.
Card Acceptor Name/Location	40	Alpha Numeric Special Char	Contains the name and location of the card acceptor (i.e. the merchant or ATM).
Card Acceptor Terminal Identification	15	Alpha Numeric Special Char	Contains a unique code identifying a terminal at the card acceptor location.
Authorization Identification Response	6	Alpha Numeric	Contains the response identification assigned by the authorizing institution. This field is often referred to as "auth-code".

Response Code	2	Alpha Numeric	Contains a code, which defines the disposition of a message.

II. PoS data:

Field Name	Max Size	Type	Field Details
Primary Account Number (PAN)	16-19	Numeric	PAN is a series of digits used to identify a Retail Payment Service User account or relationship
Transaction Code	2	Numeric	Transaction Code - 00 (Purchase/Sale), 20 (Refund), 31 (Balance Enquiry).
Transaction Amount	12	Numeric	Amount of funds requested by the cardholder.
Transaction Currency Code	3	Numeric	Code that indicates the local currency of the acquirer or source location of the transaction. This defines the currency that applies to the transaction amount.
Transmission Date and Time	10	Numeric	MMDDhhmmss format Generated and sent by the message initiator. It is expressed in GMT.
Systems Trace Audit Number	6	Numeric	Unique identifier assigned to the transaction by the message sender. It remains unchanged for all messages within a transaction between the two parties. This is used to provide an audit trail for every message sent by the acquirer for a given business date.
Merchant Category Code	4	Numeric	Contains the classification of the merchant's type of business product or service.
Acquiring Institution Country Code	3	Numeric	Contains the code of the country where the acquiring institution is located (see ISO 3166)
Point of Service Entry Mode	3	Numeric	Contains two numeric to indicate the method by which the primary account number was entered into the system and one numeric to indicate the PIN entry capabilities.
POS Condition Code	2	Numeric	Contains an identification of the condition under which the transaction takes place at the point of service. 00 - Normal Presentment 59 - eCommerce
Authorization Identification Response	6	Alpha Numeric	Contains the response identification assigned by the authorizing institution. This field is often referred to as "auth-code".

Card Acceptor Terminal ID	16	Alpha Numeric Special Char	Unique code identifying the terminals at the acquirer location

Card Acceptor Identification Code	15	Alpha Numeric Special Char	Unique code identifying the card acceptor
Card Acceptor Name and Location	40	Alpha Numeric Special Char	Used to hold the name and location of the card acceptor as known to the cardholder.
Response Code	2	Alpha Numeric	Contains a code, which defines the disposition of a message.

III. Fraud data:

Field Name	**Max Size**	**Type**	**Field Details**
Primary Account Number (PAN)	16-19	Numeric	PAN is a series of digits used to identify a Retail Payment Service User account or relationship
Transaction Code	2	Numeric	Transaction Code - 00 (Purchase/Sale), 20 (Refund), 31 (Balance Enquiry).
Transaction Amount	12	Numeric	Amount of funds requested by the cardholder.
Transaction Currency Code	3	Numeric	Code that indicates the local currency of the acquirer or source location of the transaction. This defines the currency that applies to the transaction amount.
Transmission Date and Time	10	Numeric	MMDDhhmmss format Generated and sent by the message initiator. It is expressed in GMT.
Systems Trace Audit Number	6	Numeric	Unique identifier assigned to the transaction by the message sender. It remains unchanged for all messages within a transaction between the two parties. This is used to provide an audit trail for every message sent by the acquirer for a given business date.
Merchant Category Code	4	Numeric	Contains the classification of the merchant's type of business product or service.
Acquiring Institution Country Code	3	Numeric	Contains the code of the country where the acquiring institution is located (see ISO 3166)
Point of Service Entry Mode	3	Numeric	Contains two numeric to indicate the method by which the primary account number was entered into the system and one numeric to indicate the PIN entry capabilities.
POS Condition Code	2	Numeric	Contains an identification of the condition under which the transaction takes place at the point of service. 00 - Normal Presentment

			59 - eCommerce
Authorization Identification Response	6	Alpha Numeric	Contains the response identification assigned by the authorizing institution. This field is often referred to as "auth-code".
Card Acceptor Terminal ID	16	Alpha Numeric Special Char	Unique code identifying the terminals at the acquirer location
Card Acceptor Identification Code	15	Alpha Numeric Special Char	Unique code identifying the card acceptor
Card Acceptor Name and Location	40	Alpha Numeric Special Char	Used to hold the name and location of the card acceptor as known to the cardholder.
Response Code	2	Alpha Numeric	Contains a code, which defines the disposition of a message.